MAY 2019

M.Sc. in Electrical and Electronics Engineering

JAN SHER KHAN

REPUBLIC OF TURKEY

GAZIANTEP UNIVERSITY

GRADUATE SCHOOL OF NATURAL & APPLIED SCIENCES

COMPRESSIVE SENSING AND IMAGE ENCRYPTION

M. Sc. THESIS

IN

ELECTRICAL AND ELECTRONICS ENGINEERING

BY

JAN SHER KHAN

MAY 2019

COMPRESSIVE SENSING AND IMAGE ENCRYPTION

M.Sc. Thesis

in

Electrical and Electronics Engineering

Gaziantep University

Supervisor

Associate. Prof. Dr. Sema Koç Kayhan

by

Jan Sher KHAN

May 2019

REPUBLIC OF TURKEY
GAZIANTEP UNIVERSITY
GRADUATE SCHOOL OF NATURAL & APPLIED SCIENCES
ELECTRICAL AND ELECTRONICS ENGINEERING

Name of the thesis : Compressive Sensing and Image Encryption

Name of the student : Jan Sher KHAN

Exam date : 24.05.2019

Approval of the Graduate School of Natural and Applied Sciences

Prof. Dr. Ahmet Necmeddin YAZICI
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Ergun ERÇELEBİ
Head of Department

This is to certify that we have read this thesis and that in our majority opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assoc. Prof. Dr. Sema Koç KAYHAN
Supervisor

Examining Committee Members	Signature
Assoc. Prof. Dr. Kemal DELİHACIOĞLU	……..…….…….
Asst. Prof. Dr. Serkan ÖZBAY	…….
Assoc. Prof. Dr. Sema Koç KAYHAN	…….

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Jan Sher KHAN

ABSTRACT

COMPRESSIVE SENSING AND IMAGE ENCRYPTION

KHAN, Jan Sher
M.Sc. in Electrical and Electronics Engineering
Supervisor: Assoc. Prof. Dr. Sema Koç KAYHAN
MAY 2019
47 pages

Out of various cryptographic attacks, Chosen-Plaintext Attack (CPA) is one of the most powerful and widely used attack on encrypted images. In order to efficiently resist such a strong attack, a novel chaos and Compressive Sensing (CS) based image encryption algorithm is presented in this work. Firstly, the original plaintext image is compressed via Orthogonal Matching Pursuit with Partially Known Support (OMP-PKS) and then the compressed image is confused and diffused using TD-ERCS and Skew-tent chaotic maps, respectively. Correlation among the compressed pixels is break down via confusing the image pixels using TD-ERCS chaotic map. Skew-tent chaotic map is employed for the pixel diffusion process. To get the final ciphertext image, the confused pixels are further changed through bitwise XORed operation via random matrix. For the sake of higher security, the initial conditions of chaotic maps are made dependent on the plaintext image and the parameters are computed via SHA-512. Furthermore, to decrease the transmission bandwidth, the measurement matrix is generated via Beta chaotic map. Instead of sending the whole measurement matrix, the sender will just send the Beta chaotic map initial conditions and control parameters (key) values along with the compressed ciphertext. The reliability and robustness of the designed image compression and encryption scheme are verified via experimental analysis and simulation results. All the experimental and simulation results are in favour of the proposed scheme.

Key Words: Compressive Sensing, OMP-PKS, Image Encryption, Chaos, Permutation, SHA-512.

ÖZET

SIKIŞTIRMALI ALGILAMA VE GÖRÜNTÜ ŞİFRELEME

KHAN, Jan Sher
Yüksek Lisans Tezi, Elektrik ve Elektronik Mühendisliği
Tez Yöneticisi: Doç. Dr. Sema Koç KAYHAN
Mayıs 2019
47 sayfa

Çeşitli şifreleme saldırılarından Chosen-Plaintext Attack (CPA), şifreli görüntülerde en güçlü ve en yaygın şekilde kullanılan saldırılardan biridir. Bu kadar güçlü bir saldırıya etkin bir şekilde direnmek için, bu çalışmada yeni bir kaos ve Sıkıştırıcı Algılama (SA) tabanlı görüntü şifreleme algoritması sunulmuştur. İlk olarak, orijinal düz metin görüntüsü, Kısmen Bilinen Desteğe Sahip Ortogonal Eşleştirme Pursuit (OMP-PKS) ile sıkıştırılır ve daha sonra sıkıştırılmış görüntü, sırasıyla TD-ERCS ve Skew-tent kaotik haritalar kullanılarak karıştırılır ve dağıtılır. Sıkıştırılmış pikseller arasındaki korelasyon, TD-ERCS kaotik haritası kullanılarak görüntü piksellerinin karıştırılmasıyla bozulur. Skew-tent kaotik haritası, piksel difüzyon işlemi için kullanılır. Son şifreli metin görüntüsünü elde etmek için, karışık pikseller rastgele matris aracılığıyla bit yönünde XORed işlemi ile bir defa daha değiştirilir. Daha yüksek güvenlik için, kaotik haritaların başlangıç koşulları düz metin görüntüsüne bağlı olarak yapılır ve parametreler SHA-512 ile hesaplanır. Ayrıca, iletim bant genişliğini azaltmak için, ölçüm matrisi Beta kaotik haritası ile üretilir. Tüm ölçüm matrisini göndermek yerine, gönderen, yalnızca Beta kaotik harita başlangıç koşullarını ve kontrol parametreleri (anahtar) değerlerini, sıkıştırılmış şifreli metinle birlikte gönderir. Tasarlanan görüntü sıkıştırma ve şifreleme düzeninin güvenilirliği ve sağlamlığı, deneysel analiz ve simülasyon sonuçlarıyla doğrulanır. Tüm deneysel ve simülasyon sonuçları önerilen programın lehinedir.

Anahtar Kelimeler: Sıkıştırma algılama, OMP-PKS, Görüntü şifreleme, Kaos, Permutasyon, SHA-512

ToMyParents

ACKNOWLEDGEMENTS

In the name of Allah, the Most Gracious, the Most Merciful. I would like to start by thanking Allah for giving me this opportunity to fulfill my dream to pursue Masters.

I would like to acknowledge and express my sincere gratitude to my supervisor Associate Professor Dr. Sema Koç KAYHAN for giving me the opportunity to do Master's thesis under her supervision and providing me with continued support during my research. Her immense knowledge, continuous strives to keep me at course and senses of quality in research have been of inestimable help through the time of research and for writing this thesis.

Secondly, I would be not here without the continued support of my role model, my Dad, Itbar KHAN, my ever-loving mom, Shams-ul-ZUHA, and my family members. I love you all! I would also like to thank my teacher, friend, brother, and supervisor Dr. Jawad AHMAD. Thank you for your supportive suggestions and commendable help. Thank you for being here, whenever I need you

Finally, I would like to express my appreciation to the Yurtdışı Türkler ve Akraba Toplulukları Başkanlığı for granting me this scholarship to pursue my Masters in Turkey.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

LIST OF SYMBOLS

a_1	Beta map control parameter
a_2	Beta map control parameter
B	Calculated binary value in case of NPCR
C	Contrast
$C.C$	Correlation coefficient value
c	Beta map control parameter
col	Number of columns
E	Expected value operator
E_1	Encrypted image without any change in the original image
E_2	Encrypted image with one pixel change in the original image
$\mathcal{F}$	Matrix
G	Godunov numerical flux [kg/ (m^2/ s)]
i	Number of iterations
K	Number of non-zero elements
Key	Key space value
M	Number of rows
m	TD-ERCS map control parameter
N	Number of columns
$N-K$	Number of zero elements

$\boldsymbol{n}$	TD-ERCS map control parameter
$\boldsymbol{P}$	Plaintext image
$\boldsymbol{P_i}$	Sparse image
$\boldsymbol{r_i}$	Residue vector
$\boldsymbol{R_n}$	Real numbers
$\boldsymbol{row}$	Number of rows
$\boldsymbol{S}$	Weighting coefficients in terms of column vector
$\boldsymbol{T}$	Transpose
$\boldsymbol{t}$	Skew-tent map control parameter
$\boldsymbol{u}$	Represent row-wise pixel position
$\boldsymbol{v}$	Represent column-wise pixel position
$\boldsymbol{v_i}$	Skew-tent map random numbers vector
$\boldsymbol{v_0}$	Skew-tent map initial condition
$\boldsymbol{x_{Beta}}$	Bet map control parameter
$\boldsymbol{x}$	Signal/image
$\boldsymbol{x^*}$	Represent the reconstructed image in PSNR calculation
$\boldsymbol{x_i}$	TD-ERCS map random numbers vector
$\boldsymbol{x_0}$	TD-ERCS map initial condition
$\boldsymbol{y_{Beta}}$	Bet map random control parameter
$\boldsymbol{y_{col}}$	Column permuted image
$\boldsymbol{y_{colinv}}$	Inverse column permuted image
$\boldsymbol{y_{diff}}$	XORed diffused image

$\boldsymbol{y_{diffinv}}$	Inverse XORed image
$\boldsymbol{y_i}$	TD-ERCS map random numbers vector
$\boldsymbol{y_{M.signal}}$	Compressed image or measurement signal
$\boldsymbol{y_{row}}$	Row permuted image
$\boldsymbol{y_{rowinv}}$	Inverse row permuted image or the reconstructed image
$\boldsymbol{y_{Rco}}$	Reconstructed image
$\boldsymbol{z}$	Beta map random numbers vector
$\boldsymbol{z_1}$	Beta map initial condition
$\boldsymbol{z_2}$	Beta map initial condition
$\boldsymbol{z_c}$	Beta map control parameter
μ	TD-ERCS map control parameter
$\boldsymbol{\alpha}$	TD-ERCS map control parameter
$\boldsymbol{\gamma_i}$	Highest correlation index vector
$\boldsymbol{\gamma}$	$\mathcal{F}\Delta$
$\boldsymbol{\pi_i}$	Basis index set
$\boldsymbol{\alpha_i}$	Least square value of the reconstructed signal
Δ	Column vector
$\boldsymbol{\Phi}$	Measurement matrix or sensing matrix

LIST OF ABREVIATIONS

BP	Basis Pursuit
CPU	Central Processing Unit
CS	Compressed Sensing
DWT	Discrete Wavelet Transform
E.V	Entropy value
GB	Giga Bits
GHz	Giga Hertz
GLCM	Gray Level Co-occurrence Matrix
H	Homogeneity
K-SVD	K Singular Value Decomposition
LP	Linear Programming
MSE	Mean Square Error
NPCR	Number of Pixel Change Rate
OMP	Orthogonal Matching Pursuit
OMP-PKS	Orthogonal Matching Pursuit with Partial Known support
PSNR	Peak Signal to Noise Ratio
RAM	Random Access Memory
S-Box	Substitution Box
SHA	Secure Hash Algorithm

TD-ERCS Tangent Delay Ellipse Reflecting Cavity Map System

UACI Uniform Average Change Intensity

UAVs Unmanned Air Vehicles

CHAPTER 1
INTRODUCTION

1.1 Background

Cryptography, watermarking and steganography are the fundamental three methods used for secure communication. Cryptography deals with the development of techniques for converting information between understandable and non-understandable forms during communication. Cryptography is a crucial tool for securing information systems. Cryptographic building blocks ensure the secrecy and integrity of information, and help to protect the privacy of users. Encryption is a general and secure method to defend image safety against eavesdroppers. Still, most actually deployed cryptographic schemes are not known to have any rigorously proven security guarantees. This has led to a number of far-reaching security issues in widely deployed software systems. As nowadays Internet is an easy and low cost channel for real-time information transmission and reception. Due to the open nature of Internet, threat to digital information and network technologies have been increased since last decade. To protect multimedia information from illegal copy, use and manipulation, security is a major concern in communication process. Additionally, due to the bulky size of data, sometimes we face transmission bandwidth and storage problems. Therefore, In order to provide security, protection to multimedia contents, decrease the transmission bandwidth, and required storage space, secured compressed image encryption must be developed. Traditional image encryption schemes cannot handle the emerging problems in big data such as noise toleration and compression. In order to meet today's challenges; greedy algorithm and chaos based compressed image encryption scheme is designed in this research work, which is robust to channel noise and compression.

1.2 Objectives and Contributions of the Thesis

The main objectives and Contribution of the thesis can be summarized as follows:

1. Chaos theory (nonlinear science), which is more present in our lives and surrounds than we can imagine, has been investigated and their cryptographic properties are explored and utilized to propose a compressed image encryption scheme which can withstand statistical attack, entropy attack, brute force attack, differential attack, noise attack, known-plaintext attack, cropping attack and chosen-plaintext attack.

2. Orthogonal Matching Pursuit with Partially Known Support (OMP-PKS) compressive sensing technique is used to compressed the plaintext image before encryption.

3. To decrease the transmission bandwidth and storage space, the measurement matrix is generated via chaotic map. Now, we don't need to send the whole measuring matrix to the receiver end, just the key (initial condition and parameter) values are enough.

4. Based on above two points, the main objective is to propose a strong compressed chaotic security protocols that shows good statistical analysis, resist against various differential attacks and also at the same time, transmission bandwidth and storage space can be saved.

1.3 Outline

1. From second chapter onwards, the background and literature review is discussed in detail.
2. The third chapter illustrated the proposed greed algorithm and chaos based compressed image encryption algorithm.
3. The experimental and simulation analysis of the proposed image compression and encryption scheme is presented in chapter fourth.
4. Chapter fifth concludes the research work.

CHAPTER 2
LITERATURE REIVEW

With the evolution of Internet and its related technologies, it is now possible to transmit and receive extreme larger volume of data. In literature, this larger volume of data is known as big data. Big data has applications in various industries such as banking, healthcare, energy, technology, consume and manufacturing. Despite such a wide range of applications of big data in multiple businesses, researchers are still looking for possible solutions of mainly two big challenges related to big data (i) efficient data sharing, and (ii) data privacy. The possible solutions for the aforementioned challenges include Compressive Sensing (CS) and encryption of original information. In CS technique, a signal is compressed either in its original domain or in some transformed domain for effective utilisation of bandwidth. CS can be also be defined as a measuring technique that can reconstruct images and signals from extreme fewer data/measurements. Moreover, some CS based method sparse the original signal for efficient acquisition and reconstruction of big data. In encryption, original data is transformed in such a way that an intruder has no access to original information. Encryption basically turns data into an unintelligible mess or ciphertext. That ciphertext can only be put back into a readable form by unlocking it with a key of some sort that tells the receiving body how to decode the incoming message or data.

Multimedia contents needs to be secured from different type of attacks which are interruption, interception, modification and fabrication [1, 2]. Generally speaking, security attributes are availability, confidentiality, integrity and authenticity, as shown in Fig. 2.1, which is briefly described as follows:

1. Availability: The information stored and transmitted needs to be available to authorized users; otherwise this information will be useless. Suppose user A wants to transmit a message M to user B, if an attacker blocks the flow of M to B, then M will not be available to B; as shown in Fig. 2.1 (b).

2. Confidentiality: Confidentiality means that only the intended users can see the data. It is not only required during storage of information but also required during transmission of data. Suppose A wants to transmits a message M to B but an eavesdropper E also receives the same message M. This scenario is depicted in Fig. 2.1 (c) which is an attack on the confidentiality of M.
3. Integrity: This feature provide assurance that the received message has not been altered during transmission; accidentally or intentionally. If an eavesdropper modifies the information, the integrity of the message is lost. This scenario is shown in Fig. 2.1 (d).
4. Authentication: Authentication ensures the origin and integrity of information. Figure 2.1 (e) shows an attack on the authenticity of a message. The attacker E sends a fabricated message to B, conceiving B that the message has been sent by A.

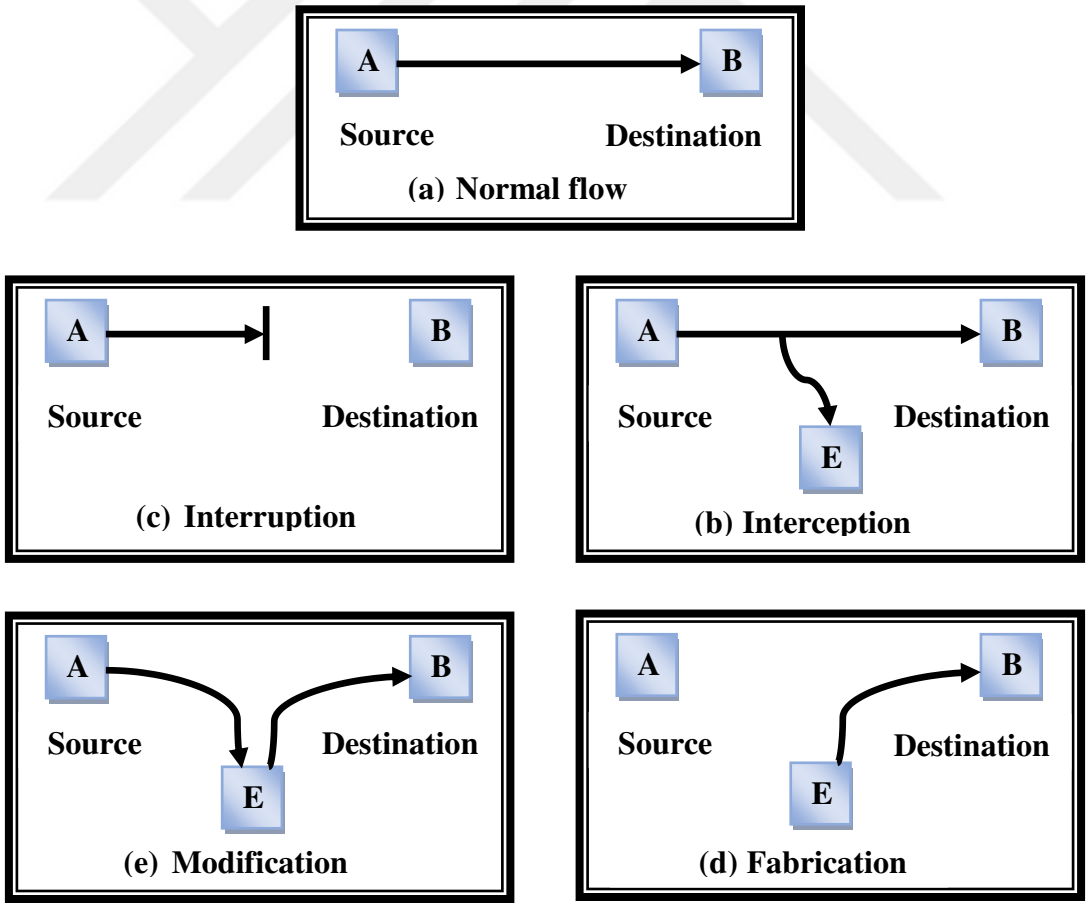


Figure 2. 1 Security attributes [1, 2].

2.1 Principles of Encryption

Encryption is basically a conversion process in which an original/plaintext message is modified in such a way that it cannot be understood by an unauthorized person. The modified/converted plaintext message is known as ciphertext. An encryption scheme has five ingredients:

(a) Plaintext
(b) Encryption algorithm
(c) Secret key
(d) Ciphertext
(e) Decryption algorithm

Usually, plaintext is represented by P and ciphertext by C. The encryption process for any cryptosystem can be defined as:

$$C = E_{k_e}(P), \tag{2.1}$$

where E is the encryption function and k_e is the encryption key. Similarly, the decryption process is defined as:

$$P = D_{k_d}(C), \tag{2.2}$$

where D is the decryption function and k_d is the decryption key. Figure 2.2 shows a block diagram of the encryption/decryption process [3] while Figs. 2.3, 2.4 and 2.5 demonstrate examples of image encryption, speech encryption, and text encryption, respectively.

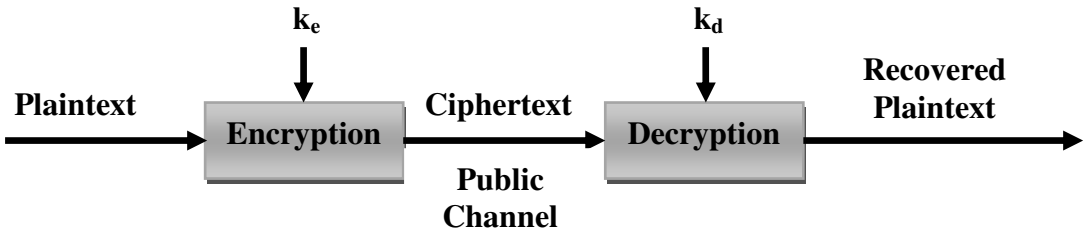


Figure 2. 2 Illustration of Encryption/Decryption process [3].

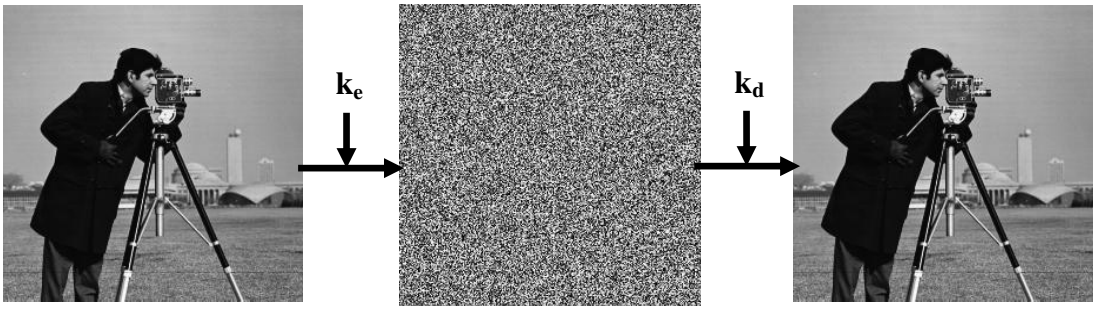


Figure 2. 3 Image encryption example.

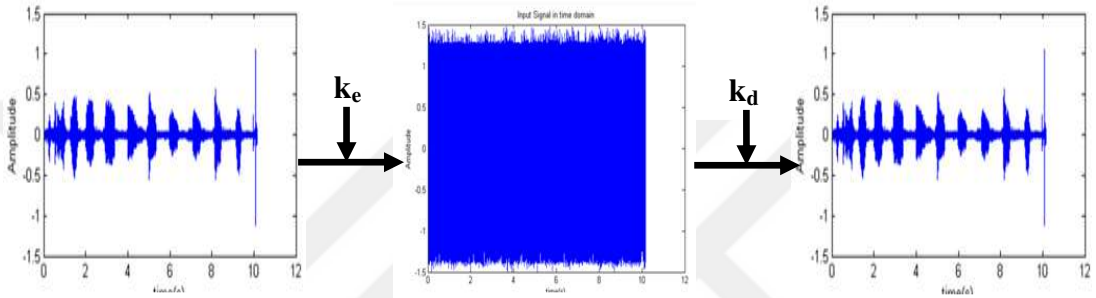


Figure 2. 4 Speech encryption example.

Figure 2. 5 Text encryption example.

2.2 Structure Based Classification of Encryption Algorithm

Structure wise image encryption scheme can be divided into block ciphers and stream ciphers. The details about these two type image encryption schemes are provided as follow:

2.2.1 Block Ciphers

In block cipher, a block of original plaintext is considered as a whole. As a result, the output is also generated as a ciphertext block. The block length for both plaintext and ciphertext remains the same. For example, for a 128-bit block of original plaintext input, a block cipher produce 128-bit ciphertext block. Being a symmetric key cipher, block cipher encrypt and decrypt all the blocks with the same key. For the sake of greater security, usually, the key size and block length are kept as large as possible. In 1977, IBM published a standard called the DES (Data Encryption Standard), which is a block cipher [1, 2].

2.2.2 Stream Ciphers

In a stream cipher, the stream of digital data is encrypted one byte or bit at a time. Autokey Venam and Vigenre are examples of stream ciphers [2]. Stream ciphers are basically used to design exceptionally faster encryption algorithms than traditional block ciphers. Stream ciphers have lower complexity compare to block ciphers [4].

2.3 Key Based Classification of Encryption Algorithm

Key wise encryption algorithms can be divided into two main types; symmetric and asymmetric key algorithms [2].

2.3.1 Symmetric Key Algorithm

If encryption is carried out in such a way that keys for encryption and decryption remain the same, then the algorithm is known as a symmetric key or private key algorithm [1, 2]. Symmetric ciphers can also be used for non-repudiation purposes and message authentication codes can also be constructed from symmetric ciphers [1, 2]. Figure 2.6 illustrates the symmetric key algorithm [5].

2.3.2 Asymmetric Key Algorithm

If encryption is carried out in such a way that keys for encryption and decryption are different, then the algorithm is known as an asymmetric key or public key algorithm [1, 2]. In the asymmetric key algorithm, the encryption key is made public so that anyone can encrypt a message, however, only the person who has the correct private key can decrypt the message. This is done for confidentiality [1, 2]. Figure 2.7 shows the asymmetric key algorithm [5].

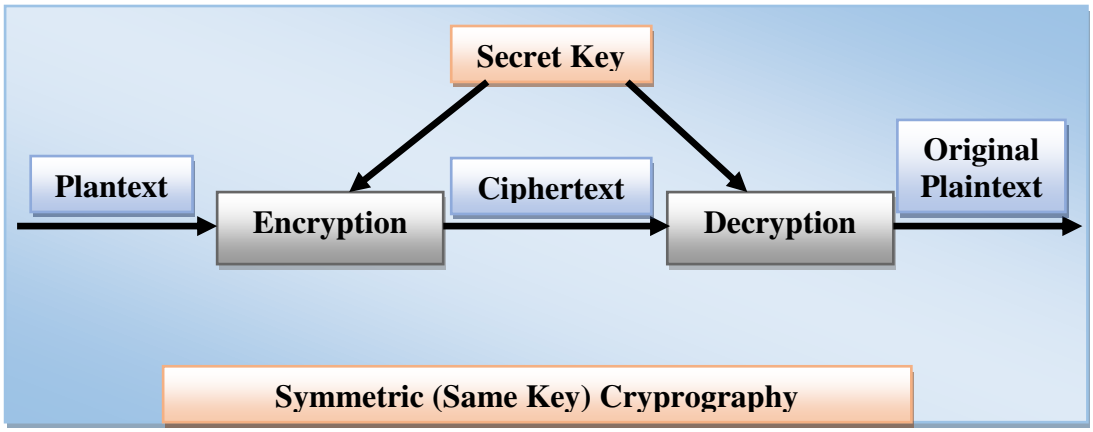


Figure 2. 6 Symmetric encryption and decryption [1, 2].

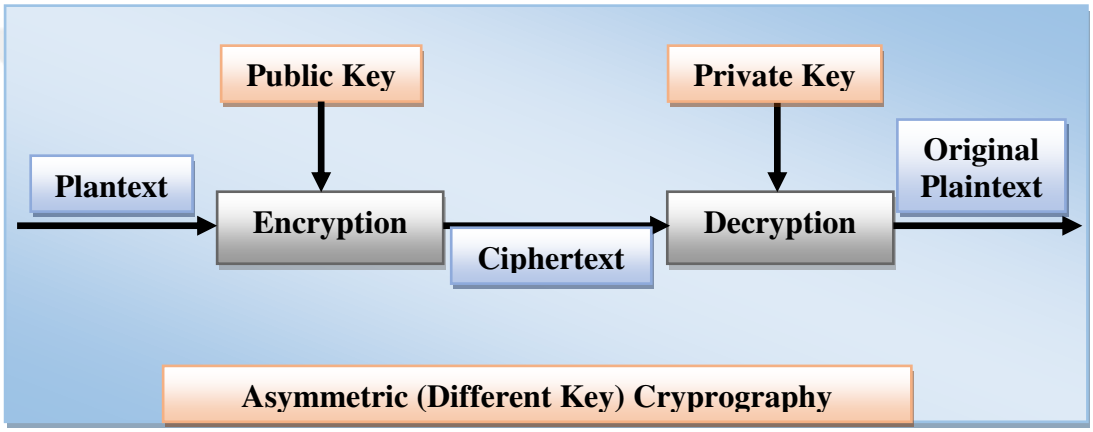


Figure 2. 7 Asymmetric encryption and decryption [1, 2].

2.4 Size Based Classification of Encryption Algorithm

Size basede image encryption schemes are categorized into two different types i. full image encryption ii., and partial image encryption.

2.4.1 Full Image Encryption Algorithm

Full image encryption deals with encrypting the entire image data and utilizes many resources and need more time for full encryption.

2.4.2 Partial Image Encryption Algorithm

Partial encryption generally need less computation and time. Moreover, partial encryption requires less resources when encrypting only region of interest in an image. Partial image encryption schemes is highly computational efficient which are

then suitable for real-time implementations and applications, such as teleconference and camera surveillance etc.

2.5 Basic Method of Encryption

There is two main methods to encrypt a message. i. confusion and ii. diffusion. Every image encryption consists of these two methods. Some researchers may design image encryption algorithms using just one of them or may change the order of application, but every scheme must consist of these two basic methods.

2.5.1 Confusion

Confusion means to confuse the plaintext image pixels. In other words, confusion means to disturb the plaintext original image pixels. Confusion also called permutation or shuffling. Confusion may be performed in three different ways.

2.5.1.1 Block Permutation

In block permutation, the plaintext image has first divided into blocks of the required size. Then these blocks are shuffled to generate a ciphertext image. Figure 2.8 illustrates the block permutation concept.

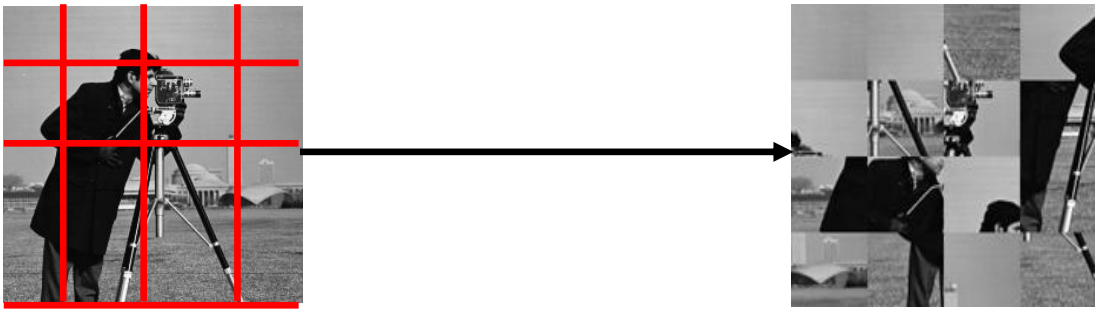


Figure 2. 8 Block permutation.

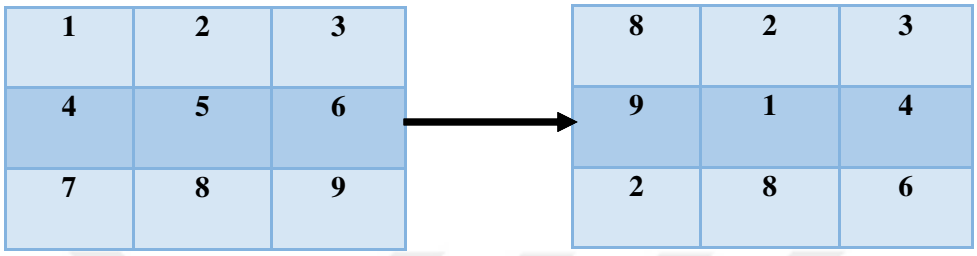
2.5.1.2 Pixel Permutation

In pixel permutation, the ciphertext image is generated via shuffling the pixel of the original plaintext image. Table 2.1 demonstrates the pixel permutation concept.

2.5.1.3 Bit Permutation

In bit permutation, the decimal values of plaintext image are first converted into binary bits string. Then those binary bits strings are confused to generate permutated ciphertext image.

Table 2. 1 Pixel permutation.



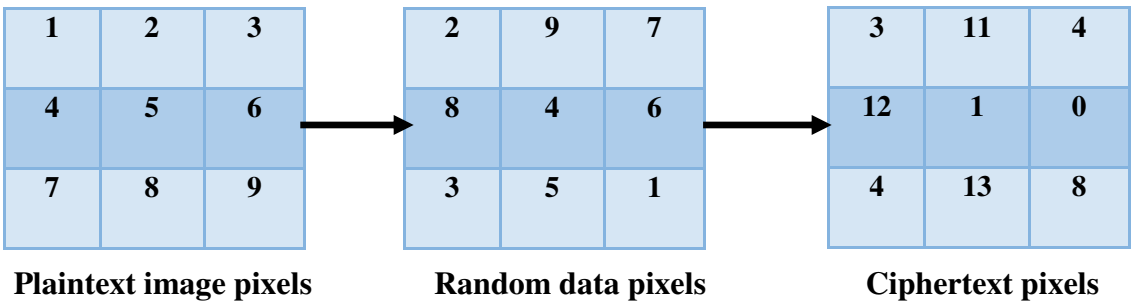
2.5.2 Diffusion

Diffusion means, replacing the original plaintext data with some other data. Diffusion may be performed in three different ways.

2.5.2.1 XOR Operation

In XOR operation, the original image pixels are bitwise XORed with some other data set to generate a diffused ciphertext image. Table 2.2 illustrated bitwise XOR concept.

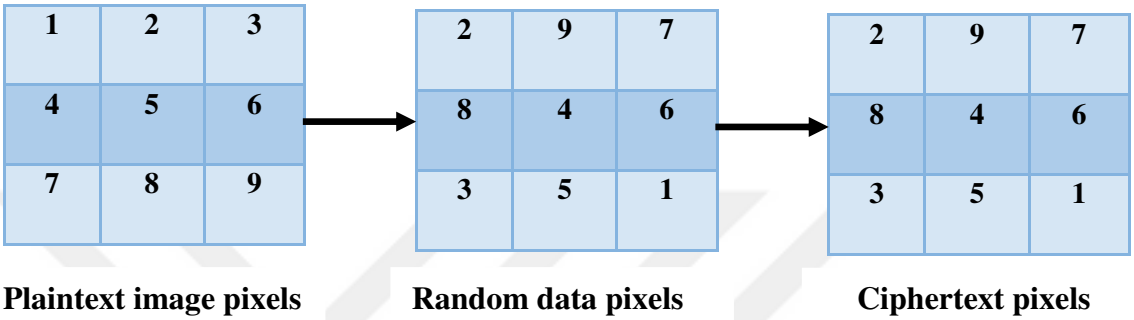
Table 2. 2 Bitwise XORed operation.



2.5.2.2 Pixel Substitution

In pixel substitution, the ciphertext is generated via substituting the original plaintext pixels with some other data matrix pixels. For example, in Table 2.3 plaintext image pixels are substitute with random matrix data. The ciphertext generated is totally different from the plaintext image data.

Table 2. 3 Pixel substitution.



2.5.2.2 Bits Substitution

In bit substitution, the decimal values of plaintext image are first converted into binary bits string. Then those binary bits strings are substitute to generate diffused ciphertext image.

Because of transmission over untrustworthy wireless channels and open natured Internet, malicious attacks and packets loss can be expected. Data can be secured from eavesdropper via encrypting. To ensure secure transmission of data, data must be encrypted before transmission. However, considering the cost and traffic load, traditional encryption schemes are not suitable for real-time encryption. Therefore, after the novel idea of Matthews about chaos-based image encryption, many researchers designed chaos based efficient and robust image encryption schemes [6]. Due to unpredictable and pseudorandom nature, sensitivity to initial conditions and control parameters chaos has been widely utilized in designing image encryption schemes [7–17]. The authors in [7] utilized a complex chaotic system to generate three different S-Boxes. The control parameters and initial conditions of the chaotic system are computed via random noise and plaintext image. This scheme can encrypt color images in a faster manner. Instead of encrypting the whole image, the authors in [8-9] encrypt selective portions of the image to reduce the computation time and

cost. The random noise like look of ciphertext attracts attacker attention. Therefore, to enhance the security of an image encryption scheme, the authors in [12-13], designed visually secure image encryption schemes using chaotic maps. The plaintext image is first encrypted via an encryption algorithm and then embedded in a carrier image to visually secure the plaintext image. Xiao et al. encrypt multi-focus fused images and decrease the transmission rate using CS [14]. Hu et al. and Chai et al. also decrease the data volume of encrypted images via introducing CS [15-16].

2.6 Compressive Sensing based Image Encryption

Compressed sensing (CS) revolutionize the concept of reconstruction via sampling the compressed signal at a rate much less than the Nyquist rate or constructing the original sparse signal from a small number of measurements as possible as it could. Due to the complex nature for many applications, Linear Programming (LP) technique based CS decoder has limited practical applications. Therefore, we need to design faster CS decoder algorithms [28]. The primary goal of the CS is to utilize the least numbers of linear measurements during the reconstruction of a highly dimensional sparse signal. Since last decade, Compressive sensing has received significant attention [20-33]. Mostly the conventional reconstructing algorithms are based on Shannon sampling theorem, which states that a signal can be sampled at a sampling rate of at least 2 times larger than the uppermost frequency [19]. The fundamental concepts i.e., sparse recovery (inferring a high dimensional signal from very few observation) by convex optimization, were identified several decades ago while the authors in [20-22], were the first to present the seminal work of compressed sensing in 2006. These articles basically underline the strong potential of compressed sensing in a number of application areas. After this, many researchers turn their attention towards compressive sensing application [23–26]. Aharon et al. accomplish sparse signal representations via adapting dictionaries and design K-Singular Value Decomposition (K-SVD) algorithm [23]. The authors in [24-25], utilize sparse signal representation to automatically recognize human faces. Li et al. present video-based action retrieval and classification by utilizing sparse signal representation [26]. Vishal et al. prove that the synthetic aperture for radar imaging can be compressed utilizing CS theorem [27]. The authors in [28], proved theoretically and empirically that Basis Pursuit (BP) can be effectively replaced via OMP. They also considerably decrease the theoretical performance gap between

Linear Programming (LP) and greedy algorithms. Davenport et al. show that the OMP can be analyzed effectively via Restricted Isometry Property (RIP) [29]. The authors in [30], reduce the computing time and storage memory via dividing the image into *n x n* pixels blocks and then applying OMP to those blocks instead of the complete image. Gibson et al. use CS concepts to design an intelligent fall detection system [31]. Gibson et al. system uses a database consists of fall and daily life activities to attain binary tree classifier for fall detection via principal component analysis and discrete wavelet transform. The authors in [32], introduce CS in microwave imaging technology via retrieving arbitrary shaped targets. The authors in [33], improve the image quality of the compressive line sensing system for Unmanned Aired Vehicles (UAVs) application via combining distributed and dynamic compressive sensing.

As mentioned earlier, CS and encryption of original information are the possible solution for two big challenges related to big data (i) efficient data sharing, and (ii) data privacy. Therefore, rmany researchers turn their attention to design CS based compressed image encryption schemes [14-16]. Xiao et al. encrypt multi-focus fused images and decrease the transmission rate using CS [14]. Initially, the human eye perception optimization and complete scene images are generated via multi-focus image fusion using wavelet decomposition. In the next stage, to reduce the initial data volume, the fused images are sparsified using DCT and Strucuturally Random Matrix (SRM). Finally, the compressed image is encrypted to assure noise and crop attack resistance. The authors in [15] designed a novel image encryption scheme via combining encryption and compression under a parallel compressive sensing framework. The parallel nature of CS sampling and reconstruction guarantee the efficiency. The scheme is made resistant against chosen plaintext attack (CPA) through nonlinear chaotic sensing matrix generaion. Diffusion is also induced to overcome the energy information defect in CS–based cryptosystems. Chai et al. also decrease the data volume of encrypted images via introducing CS and decrease the number of attacks on the ciphertext by embedding it into a carrier image [16]. Wavelet coeffiecients are used to transformed the original plaintext image into wavelet coeffiecients. Then the wavelet coefficients are encrypted using zigzag path confusion. In the next stage, the encrypted image is compressed using compressive sensing. Finally, the cipher image is embedded into a host image to generated

visually secure ciphertext. The chatic parameters are computed via passing the plaintext image through SHA-256 hash fuction, which makes the scheme strong enough to withstand known-plaintext and chosen-plaintext attacks effectively.

Let say we have a single dimensional, real-valued, finite-length, discrete time, *K-sparse* signal *x* with *K* non-zero elements and *(N - K)* zero elements. Signal *x* is basically *Nx1* vector in R^N i.e., *x[i], i = 1, 2, 3, ..., N.* In the case of higher dimensional data or images, the data can be converted or written in a single dimensional vector. For simplicity purpose, we assume that the basis are orthonormal. Therefore, utilizing the *N x N* basis matrix $\Delta = [\Delta_1 \mid \Delta_2 \mid \Delta_3 \mid \ldots \mid \Delta_N]$, where Δ_n represents a column vector. Now mathematically the signal *x* can be computed as:

$$x = \sum_{n=1}^{N} S_n \Delta_n \tag{2.3}$$

$$x = \Delta S \tag{2.4}$$

After rearranging Eq. (2.4), we have

$$S_n = < x, \Delta_n > \tag{2.5}$$

$$S_n = \Delta_n^T x \tag{2.6}$$

where *S* represents weighting coefficients in term of a column vector and *T* demonstrates the transpose. Suppose we have a linear measurement process as follows:

$$y_i = < x, \Phi_i > \tag{2.7}$$

Equation (2.7) is actually $M < N$ times inner product between *x* and vector $\{\Phi_i\}_{i=1}^{M}$. y_i is a column vector of size *M x 1* and Φ_i^T represent the number of rows in a matrix *z* of size *M x N*. Now substitute Eq. (2.4) into (2.7).

$$y = \mathcal{F}x \tag{2.8}$$

$$y = \mathcal{F}\Delta S \tag{2.9}$$

$$y = \gamma S \tag{2.10}$$

2.7 Chaotic Maps

Due to unpredictable and pseudo-random nature, sensitivity to initial conditions and control parameters, three different chaotic maps are used in our proposed OMP-PKS and chaos-based compressed image encryption scheme. The details about those maps are provided as follows:

2.7.1 Beta Maps

The authors in [34], introduced a new map to the chaotic family in 2017. Mathematically Beta chaotic map can be computed as:

$$z_{n+1} = t \times Beta(z_n; x, y, z_1, z_2) \tag{2.11}$$

Where

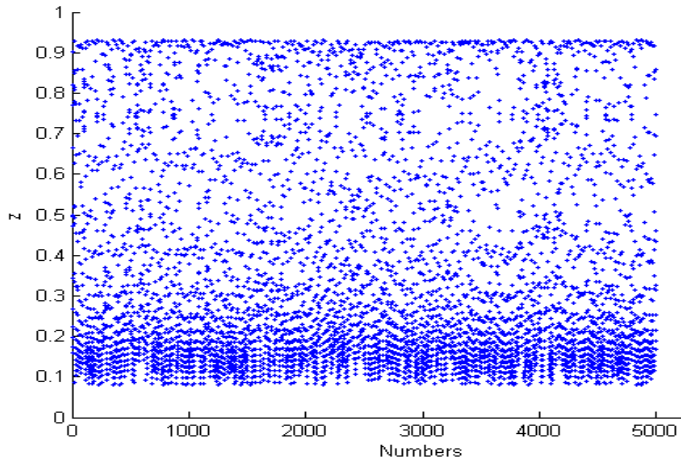
$$Beta(z_n; x, y, z_1, z_2) = \begin{cases} \left(\frac{z - z_1}{z_c - z_1}\right) x \left(\frac{z_2 - z}{z_2 - z_c}\right) y & if z \epsilon (z_1, z_2), \\ 0 & if\ otherwise. \end{cases}$$

$$x = k_1 + a_1 \times c$$

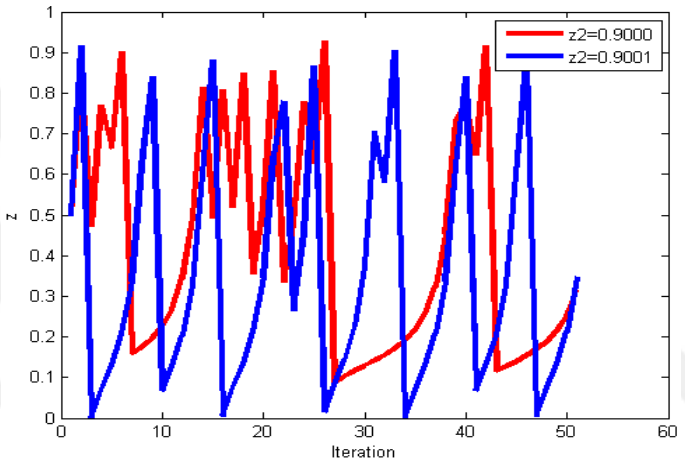
$$y = k_2 + a_2 \times c$$

$$z = \frac{xz_2 + yz_1}{x + y}$$

x, y, z_1 and *z_2* are constants and $\epsilon\ R_n$ with $z_1 < z_2$ and *c* demonstrates the bifurcation parameter and *t* controls the amplitude of Beta chaotic map. The distribution of 5000 random numbers via Beta chaotic map for parameters *c = [-0.4, 0.7], z_1 = 0.7, z_2 = 1, t = 0:93, k_1 = 8, k_2 = 3, a_1 = 1* and *a_2 = -1* is shown in Fig. 2.9(a). One can also see from Fig. 2.9(b), that a small change in one of the initial condition results in the generation of total different random numbers. Thus Figs. 2.9(a) and 2.9(b) confirm the chaotic nature of Beta chaotic map.



(a)



(b)

Figure 2. 9 Random number plots of Beta chaotic map: (a) Distribution of random numbers z (b) Random numbers for slightly different values of z_0.

2.7.2 TD-ERCS Maps

Utilizing the physical model of ellipse reflecting cavity, Prof. Yuan Sheng Lee in 2004 developed 2-D chaotic system known as Tangent Delay Ellipse Reflecting Cavity Map System (TD-ERCS Map) [35]. Mathematically TD-ERCS map can be computed as:

$$x_n = \frac{(2L_n y_{n-1} + x_{n-1}(\mu^2 - L_{n-1}^2))}{(\mu^2 - L_{n-1}^2)} \tag{2.12}$$

$$y_n = L_{n-1}(x_n - x_{n-1}) + y_{n-1} \tag{2.13}$$

where

$$L_n = \frac{(L'_{n-m} - L_{n-1} + L_{n-1}(L'_{n-m})^2)}{(1 + 2L'_{n-m}L_{n-1} - L(L'_{n-m})^2)},$$

$$L'_{n-m} = \begin{cases} -\left(\frac{x_{n-1}}{y_{n-1}}\right) \times \mu^2 & if\ n < m, \\ -\left(\frac{x_{n-m}}{y_{n-m}}\right) \times \mu^2 & if\ n \geq m. \end{cases}$$

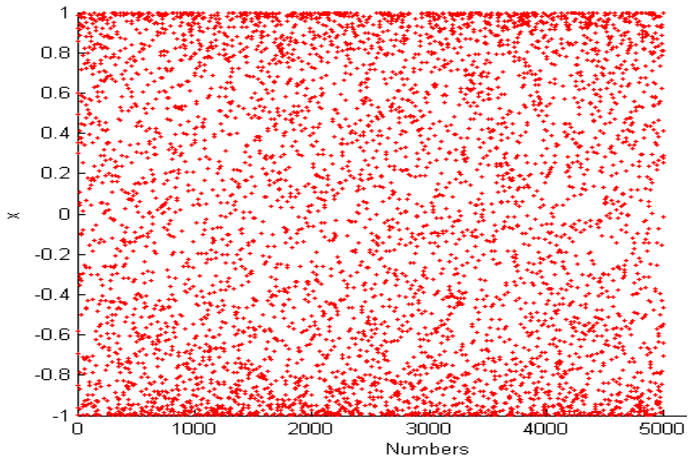
$$y_0 = (1 - x_0^2)^{\frac{1}{2}} \times \mu,$$

$$L'_0 = \left(\frac{x_0}{y_0}\right) \times \mu^2,$$

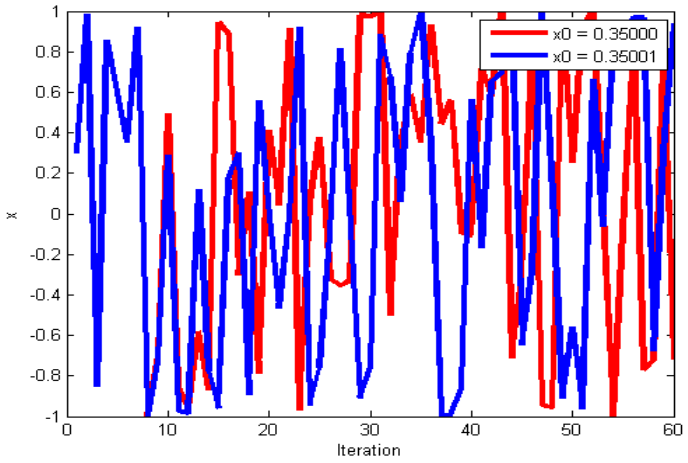
$$L_0 = -\frac{(L'_0 + \tan(\alpha))}{(1 - L'_0 \tan(\alpha))},$$

$$\begin{cases} x_0 \in [-1,1], \\ \mu \in (0,1), \\ \alpha \in (0,\pi), \\ n = 1,2,3,\ldots, \\ m = 2,3,4,\ldots. \end{cases}$$

In the above equation x_0, α, n, and m represent the seed parameters of TD-ERCS chaotic map. The distribution of 5000 random numbers via TD-ERCS chaotic map for parameters $x_0 = 0.3500$, $\alpha = \pi/4$, $\mu = 0.6$ and $m = 5$, is shown in Fig. 2.10(a). One can also see from Fig. 2.10(b), that a small change in one of the initial condition results in the generation of total different random numbers. Thus Figs. 2.10(a) and 2.10(b) confirm the chaotic nature of TD-ERCS chaotic map.



(a)



(b)

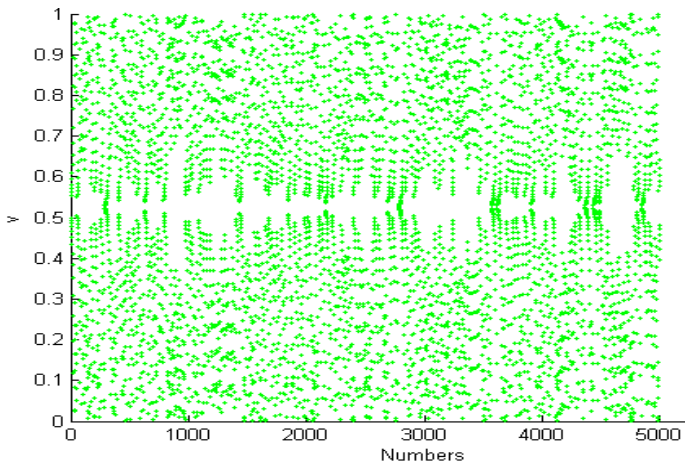
Figure 2. 10 Random number plots of TD-ERCS chaotic map: (a) Distribution of random numbers x (b) Random numbers for slightly different values of x_0.

2.7.3 Skew-tent Maps

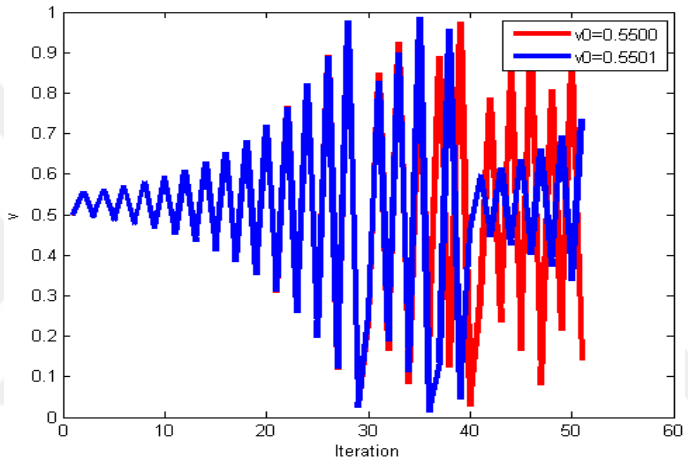
Due to positive Lyapunov exponent and ease of computation, Skew tent chaotic map can be found in many security applications [36]. Mathematically Skew-tent chaotic map can be computed as:

$$v_{i+1} = \mathcal{F}(v,t) = \begin{cases} \frac{v_i}{t} & if\ 0 < v_i < t, \\ \frac{1-v_i}{1-t} & if\ t < v_i < 1. \end{cases} \tag{2.14}$$

In Eq. *3.11*, $t \in (0, 1)$ represent the control parameter of the Skew-tent chaotic map. The distribution of 5000 random numbers via Skew-tent chaotic map for parameters $v_0 = 0.5500$, and $t = 0.1$, is shown in Fig. 2.11(a). One can also see from Fig. 2.11(b), that a small change in one of the initial condition results in the generation of total different random numbers. Thus Fig. 2.11(a) and 2.11(b) verified the chaotic nature of Skew-tent chaotic map.



(a)



(b)

Figure 2. 11 Random number plots of Skew-tent chaotic map: (a) Distribution of random numbers v (b) Random numbers for slightly different values of v_0.

CHAPTER 3
PROPOSED SCHEME

General diagram of the proposed greedy algorithm and chaos-based compressed image encryption scheme is shown in Fig. 3.1. Thus it can be easily inferred from Fig. 3.1, that the plaintext image is first compressed via OMP-PKS greedy algorithm and later on the same compressed image is encrypted. While reconstructing the plaintext image form the ciphertext image, the ciphertext image first undergoes the decryption process followed by the reconstruction phase. The detailed flowchart of the proposed scheme is demonstrated in Fig. 3.2. The proposed scheme can be concluded in the following main steps: (1) parameters computing; (2) sparse representation of the plaintext images; (3) compression via OMP-PKS; (4) chaos-based encryption; (5) decryption; (6) reconstruction of the plaintext image.

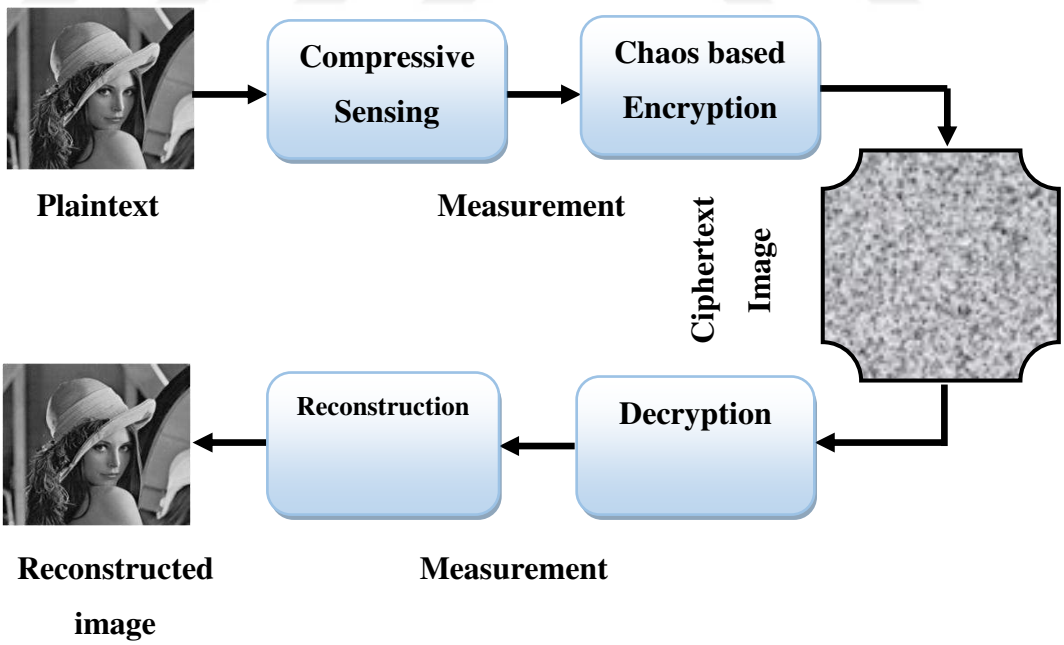


Figure 3. 1 General diagram of the proposed scheme.

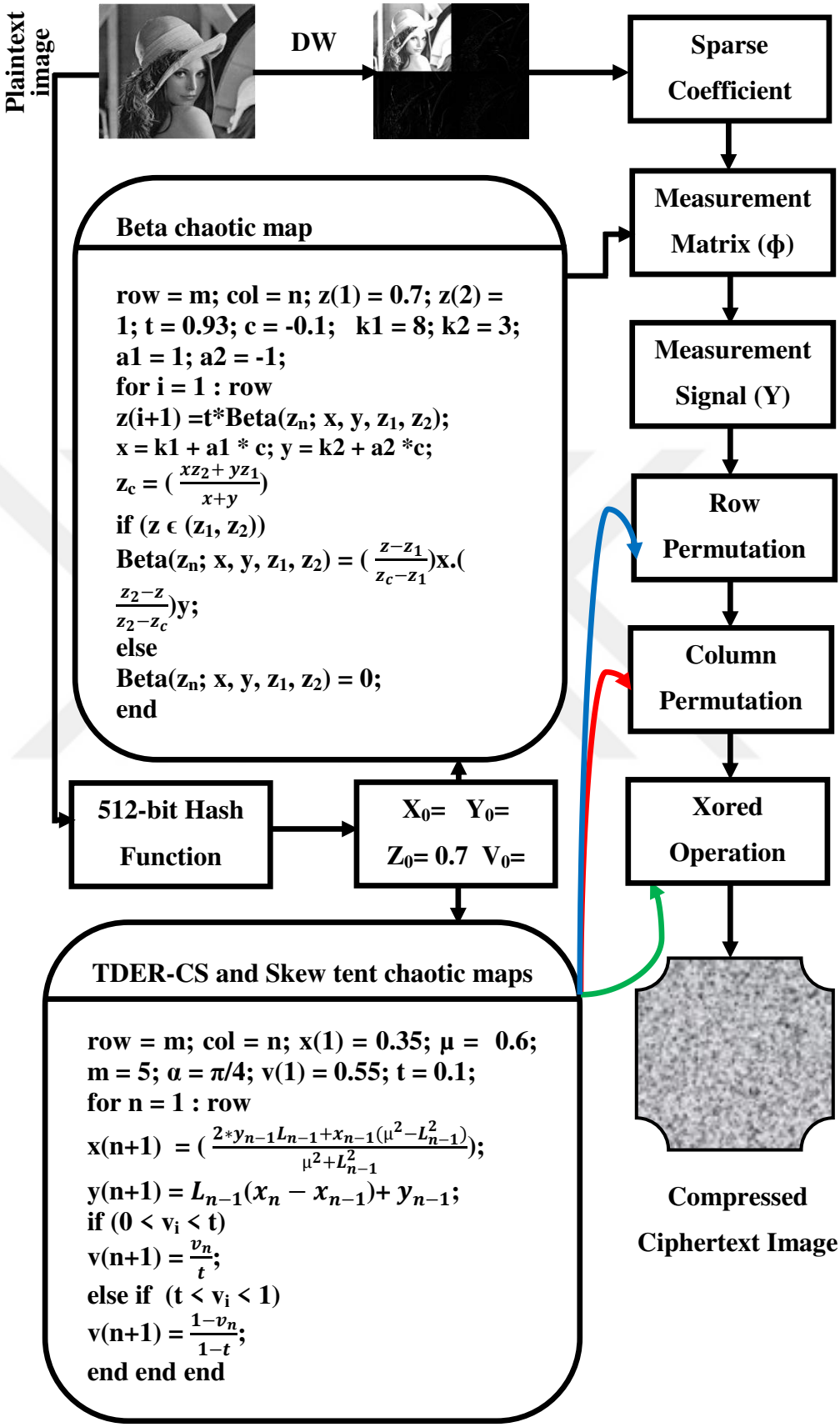


Figure 3. 2 Flow diagram of the designed image compression and encryption scheme.

3.1 Parameters Computing

The related information of plaintext image P of size *m x n* are used to obtain the initial conditions. The plaintext image is passed through the *SHA-512* hash algorithm and a *128-bytes (512-bits)* key (*Key*) is obtained. This generated secret key is then utilized to compute the final values of z_0, x_0, y_0 and v_0.

$$Key = SHA - 512(P), \tag{3.1}$$

$$z_0 = \frac{K(1:32)}{2^{130}}, \tag{3.2}$$

$$x_0 = \frac{K(33:64)}{2^{130}}, \tag{3.3}$$

$$y_0 = \frac{K(65:96)}{2^{130}}, \tag{3.4}$$

$$v_0 = \frac{K(97:128)}{2^{130}}. \tag{3.5}$$

3.2 Sparse Representation

Discrete Wavelet Transform (DWT) is used to sparsify the plaintext image *P*. The resultant coefficients are stored in matrix *P1* of size *m x n*.

$$P_1 = DWT(P). \tag{3.6}$$

3.3 Compression via OMP-PKS

Beta chaotic map is utilized to generate the sensing matrix. Beta chaotic map fulfills all the statistical properties and cryptographic features, required for an efficient and robust cryptographic system. As $y \in R^M$ is the compressed measurement signal, where *M* represent the size of sensing matrix. Therefore, Eq. 2.11 is iterated *M x n* times to compute the sensing matrix Φ.

$$\Phi = \begin{pmatrix} z_{11} & z_{11} & z_{11} & \dots & z_{11} \\ z_{11} & z_{11} & z_{11} & \dots & z_{11} \\ z_{11} & z_{11} & z_{11} & \dots & z_{11} \\ \vdots & \vdots & \vdots & & \vdots \\ z_{11} & z_{11} & z_{11} & \dots & z_{11} \end{pmatrix}. \tag{3.7}$$

Now this measurement matrix or sensing matrix Φ is utilized to generate the final compressed image or measurement signal *y*.

$$y_{M.\ signal} = \Phi P_1. \tag{3.8}$$

3.4 Chaos-Based Encryption

The compressed pixels positions are disturbed row- and column-wise via two random vectors *x* and *y*, respectively. The random vectors *x* and *y* are obtained through iterating Eq. 2.12 and 2.13 of TD-ERCS chaotic map *M x n*. Mathematically the row and column permutation can be summarized as follows:

$$y_{row} = Row_{Per}\,(y_{M.\ signal}, x). \tag{3.9}$$

$$\mathrm{y_{col}} = \mathrm{Col_{Per}}\,(\mathrm{y_{row}}, \mathrm{y}). \tag{3.10}$$

To make the scheme more secure and change the pixels values completely, the permuted image is bitwise XORed with the random matrix *v*. The random matrix *v* is obtained via iterating Eq. 2.14 of Skew-tent chaotic map *M x n*. Mathematically the diffusion step can be written as:

$$y_{diff} = bitxor(y_{col}, v). \tag{3.11}$$

This y_{diff} is the final required compressed encrypted image.

3.5 Decryption

Decryption is generally defined as the reverse process of encryption. To obtain the original image from the compressed ciphertext image y_{diff}, y_{diff} must undergo the entire encryption step in reverse order. y_{diff} is first inverse bitwise XORed with the random matrix *v* to get $y_{diff\text{-}inv}$. The inverse diffuse image $y_{diff\text{-}inv}$ is now column-wise inversely permuted followed by inverse row-wise permutation to get the original measurement matrix or compressed image $y_{M.\ signal}$. Mathematically the decryption step can be represented as follows:

$$y_{diff_{\ inv}} = bitxor\left(y_{diff}, v\right). \tag{3.12}$$

$$y_{col_{\ inv}} = Col_{Inv_{Per}}\left(y_{diff_{\ inv}}, y\right). \tag{3.13}$$

$$y_{row_{\ inv}} = Row_{Inv_{Per}}\left(y_{col_{\ inv}}, x\right). \tag{3.14}$$

where $y_{row\text{-}inv}$ is the measurement signal or the compressed signal $y_{M.\ signal}$.

3.6 Reconstruction

OMP-PKS is a modification to classical OMP via keeping the more important signal components non-zeros. Generally the lowest wavelet coefficients are elected to act as prior support information [18]. OMP-PKS utilizes low number of measurements to reconstruct the signal y as compared to OMP.

1: *i* should be incremented (*i.e., i = i+1*) and the algorithm must be broken if $i > K$.

2: Compute index γ_i for highest correlation basis Φ_j with the residual value of the last iteration r_{i-1}.

$$\gamma_i = argmax_i = [1,n]_{,j\notin\gamma_i} \left|\langle r_i, \Phi_j \rangle\right|. \tag{3.15}$$

3: Selected basis index set and its corresponding matrix must be increases.

$$\pi_i = \pi_{i-1} \cup \{\gamma_i\}. \tag{3.16}$$

$$\Phi_j = \left[\Phi_{i-1}\Phi_{\gamma_i}\right]. \tag{3.17}$$

4: Least square value for the reconstructed signal α_i must be computed.

$$\alpha_i = argmax_\alpha = \|y - \Phi_i\alpha\|_2. \tag{3.18}$$

5: The final new approximation y_{Rco} and residue r_i can be computed as:

$$y_{Rco\,(i)} = \Phi_i\alpha_i. \tag{3.19}$$

$$r_i = y_i - y_{Rco\,(i)}. \tag{3.20}$$

where $K=16$, represents the sparsity level, Φ demonstrates the chaos-based measurement matrix, y_{Rco} illustrated the reconstructed image, and π is the set with K non zero indices in y_{Rco}.

CHAPTER 4
EXPERIMENTAL EVALUTION OF THE PROPOSED SCHEME

In this section different experimental test and simulation analysis are performed to evaluate and verify the efficiency, security, and robustness of the proposed OMP-PKS and chaos-based compressed image encryption scheme. All the tests are performed on MATLAB 2013a, on a workstation with an Intel Core i3-380M CPU running at 2.53 GHz and 4.0 GB RAM. Barbara, Boat, Pepper and Goldhill images with sizes 256 x 256 are used during the analysis. The encryption results of the proposed scheme are demonstrated in Figs. 4.1. Thus one can confirm the better encryption and reconstruction results from Fig. 4.1. As shown in Fig. 4.1, the ciphertext images have a smaller size than the original plaintext images and the decrypted images have the same size as that of original plaintext images. Thus the proposed scheme has the ability to minimize the required transmission bandwidth and storage capacity. The detailed analysis is done as follows:

4.1 Statistical Attack Analysis

4.1.1 Correlation Coefficient Analysis

Generally, the adjacent pixels of an image are strongly correlated. Therefore, for any image encryption scheme, the resultant compressed ciphertext image should be totally uncorrelated and different from the plain image. Confusion performance is also evaluated via this test. For 5000 random pixels of Barbara image, the correlation coefficient values for adjacent pixels in vertical, horizontal and diagonal directions are computed using the following equations [37].

$$C.C = \frac{\frac{1}{M}\sum_{j=1}^{M}\left(u_j - E(u)\right)\left(v_j - E(v)\right)}{\sqrt{\frac{1}{M}[\sum_{j=1}^{M}\left(u_j - E(u)\right)^2 \times \sum_{j=1}^{M}\left(v_j - E(v)\right)^2]}} \tag{4.1}$$

The computed correlation coefficient values are listed in Table 4.1. The correlation coefficient values for the plain and reconstructed images are almost close to one

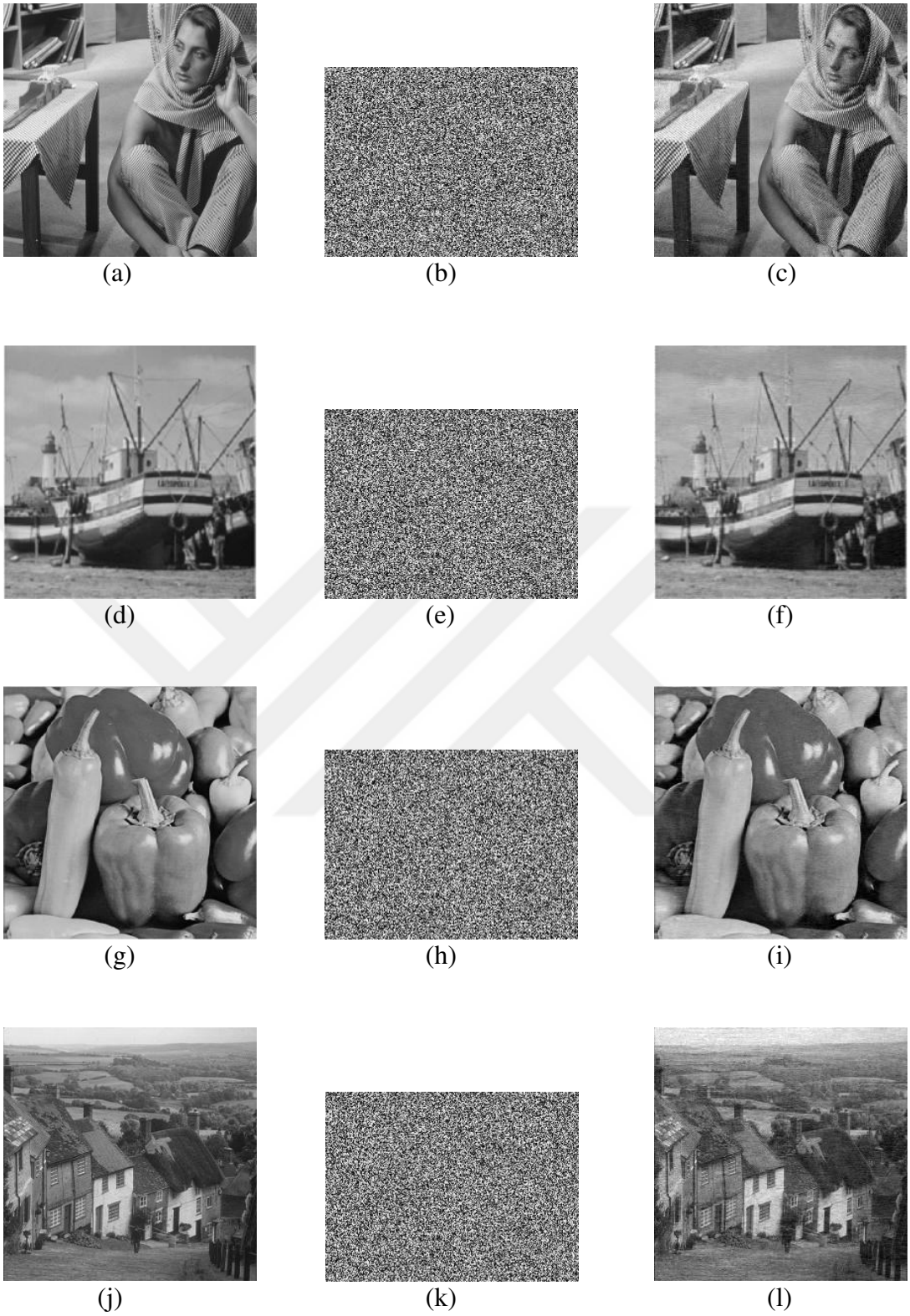


Figure 4. 1 Encryption performance: column (1) is plaintext, Barbara, Boat, Pepper, and Goldhill images, respectively; column (2) is their corresponding compressed ciphertext images; column (3) is the respective reconstructed images.

while for the cipher images it's almost zero are less than zero. Similarly, Fig. 4.2 demonstrates the pixels distribution of plain Barbara and cipher Barbara images in the coordinate system. It is clear that the correlation is disrupted to a random pattern and no detectable correlation exists. Thus the proposed image compression and encryption scheme can efficiently withstand the statistical attack.

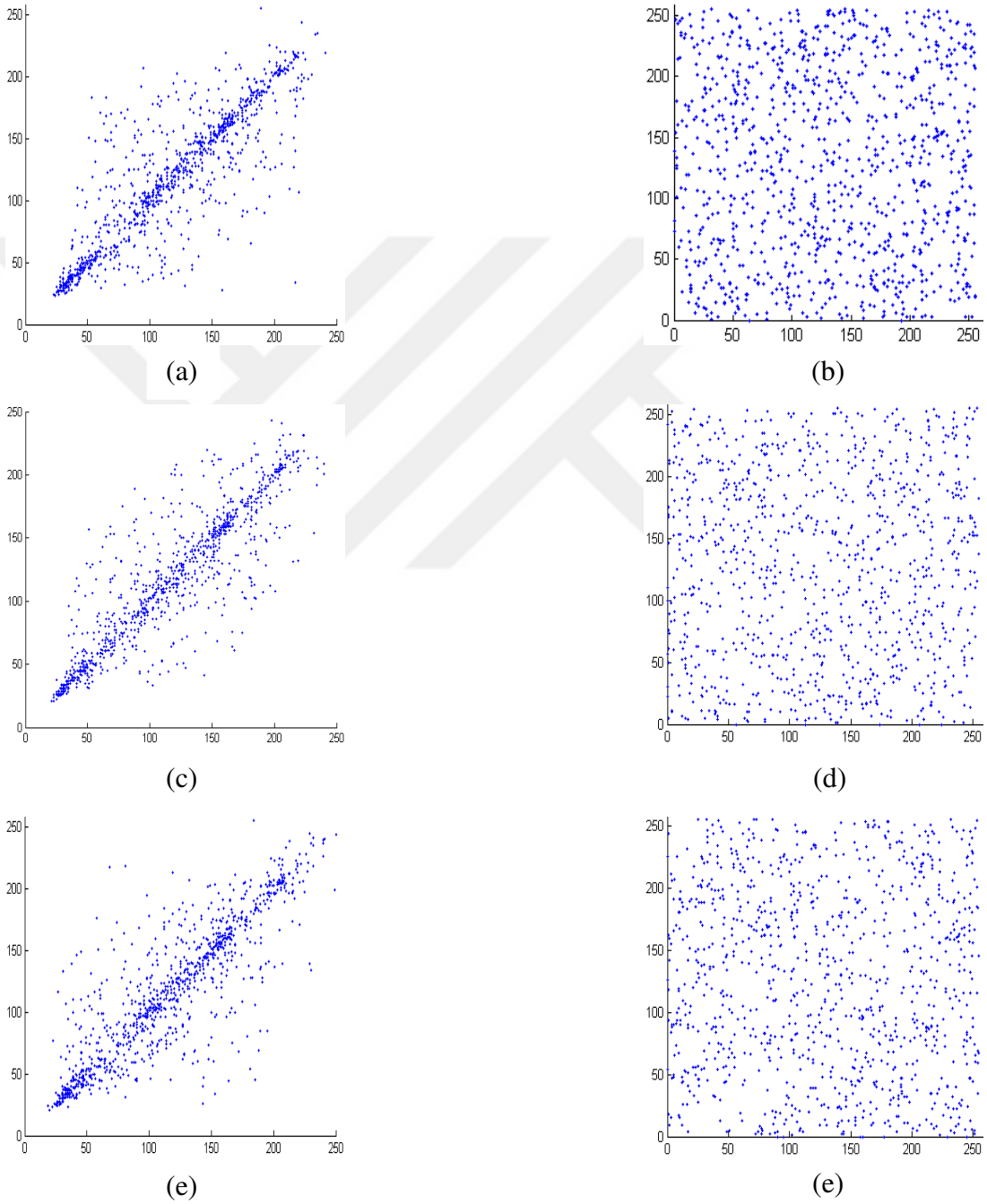


Figure 4. 2 Correlation plots of the plaintext (column 1) and ciphertext (column 2) Barbara image in (a) horizontal, (b) vertical (c) and diagonal directions, respectively.

Table 4. 1 Correlation coefficient values.

Image	Direction	Plaintext	Ciphertext	Rec-Image
Barbara	Horizontal	0.8362	-0.0085	0.8305
	Vertical	0.8770	-0.0307	0.8767
	Diagonal	0.8568	-0.0439	0.8557
Boat	Horizontal	0.9732	0.0232	0.9662
	Vertical	0.9764	-0.0130	0.9715
	Diagonal	0.9491	-0.0283	0.9394
Pepper	Horizontal	0.9695	-0.0019	0.9681
	Vertical	0.9743	0.0579	0.9732
	Diagonal	0.9298	-0.018	0.9052
Goldhill	Horizontal	0.9450	-0.0174	0.9309
	Vertical	0.9245	-0.0261	0.9122
	Diagonal	0.8967	0.0087	0.8929

4.1.2 Histogram Analysis

Histogram test is used to find how strong or efficiently, the image encryption scheme can resist statistical attack. As the histogram illustrates the distribution of pixel values in an image. Therefore, a good and secure image encryption scheme must ensure that the histogram of resultant ciphertext images has uniform distribution. The resultant ciphertext histogram of Barbara, Boat, Pepper, and Goldhill for the proposed image compression and encryption scheme are respectively shown in Fig. 4.3 (column 2). Thus it is confirmed that the resultant ciphertext histograms are uniformly distributed and do not reveal any useful information to the adversary. Therefore, the designed image compression and encryption scheme can withstand the statistical attack.

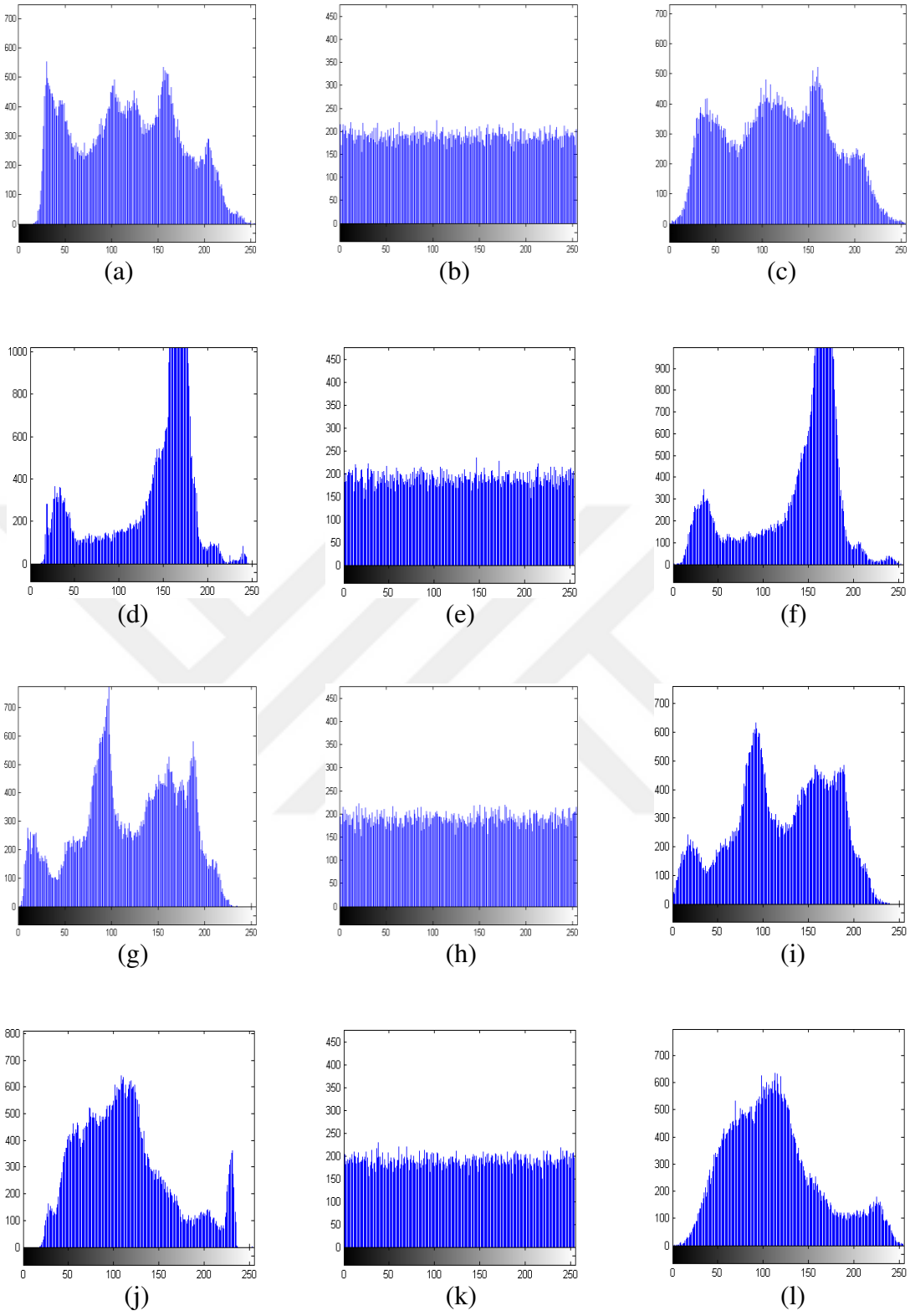


Figure 4. 3 Histogram plots: column (1) is plaintext, Barbara, Boat, Pepper, and Goldhill hitograms, respectively; column. (2) is their corresponding compressed ciphertext histograms; column (3) is the respective reconstructed histograms.

4.2 Key Analysis

4.2.1 Key Space

Key space analysis determines how strongly the cryptosystem can resist the brute force attack. A cryptosystem with key space at minimum 2^{100} can withstand the brute force attack efficiently [38]. The proposed cryptosystem secret keys consist of: (1) the initial conditions and control parameters of all the utilized chaotic maps i.e., (z_0, z_1, t_{beta}, c, x_0, α, μ, m, v_0 *and* t_{Skew}); (2) the 512-bit hash value. Without considering the hash value, the key space for the proposed scheme for computational precision 10^{-15} can be computed as:

$$K = 10^{15*10},$$
$$K = 10^{150}, \tag{4.2}$$
$$K = 2^{498.33}.$$

Thus the computed key space for the designed image compression and encryption scheme is large enough to fail any brute force attack.

4.2.1 Key Sensitivity

In differential attack, the attacker makes a small alteration in the plaintext image to see a meaningful relationship with the corresponding ciphertext image. Therefore, for a particular image encryption scheme, the resultant ciphertext should be different for a small change in the keys. Thus, this small mismatch between the keys causes the decryption failure. Therefore, key sensitivity is a critical feature and the cryptosystem should be extremely sensitive to a minute variation in the key.

In our designed image compression and encryption scheme, three chaotic maps with parameters (z_0, z_1, t_{beta}, c, x_0, α, μ, m, v_0 *and* t_{Skew}) are utilized. These parameters act as secret keys. To assess the key sensitivity, one of the above parameters is slightly changed i.e., $z_0 = 0.7 + 10^{15}$ and the encryption is repeated. The resultant ciphertext image with original keys, changed keys and their differential image along with their corresponding histograms are demonstrated in Fig. 4.4. As can be seen from Fig. 4.4, that with different keys, the proposed image encryption scheme generates different cipher image. Similarly, the decryption and reconstruction are performed with the original and modified keys and their results are illustrated in Fig. 4.5. Thus, it can be

concluded that all decrypted and reconstructed images with incorrect keys are totally unrecognizable and unable to reveal any understandable information about the plaintext images. Therefore, the proposed image compression and encryption scheme

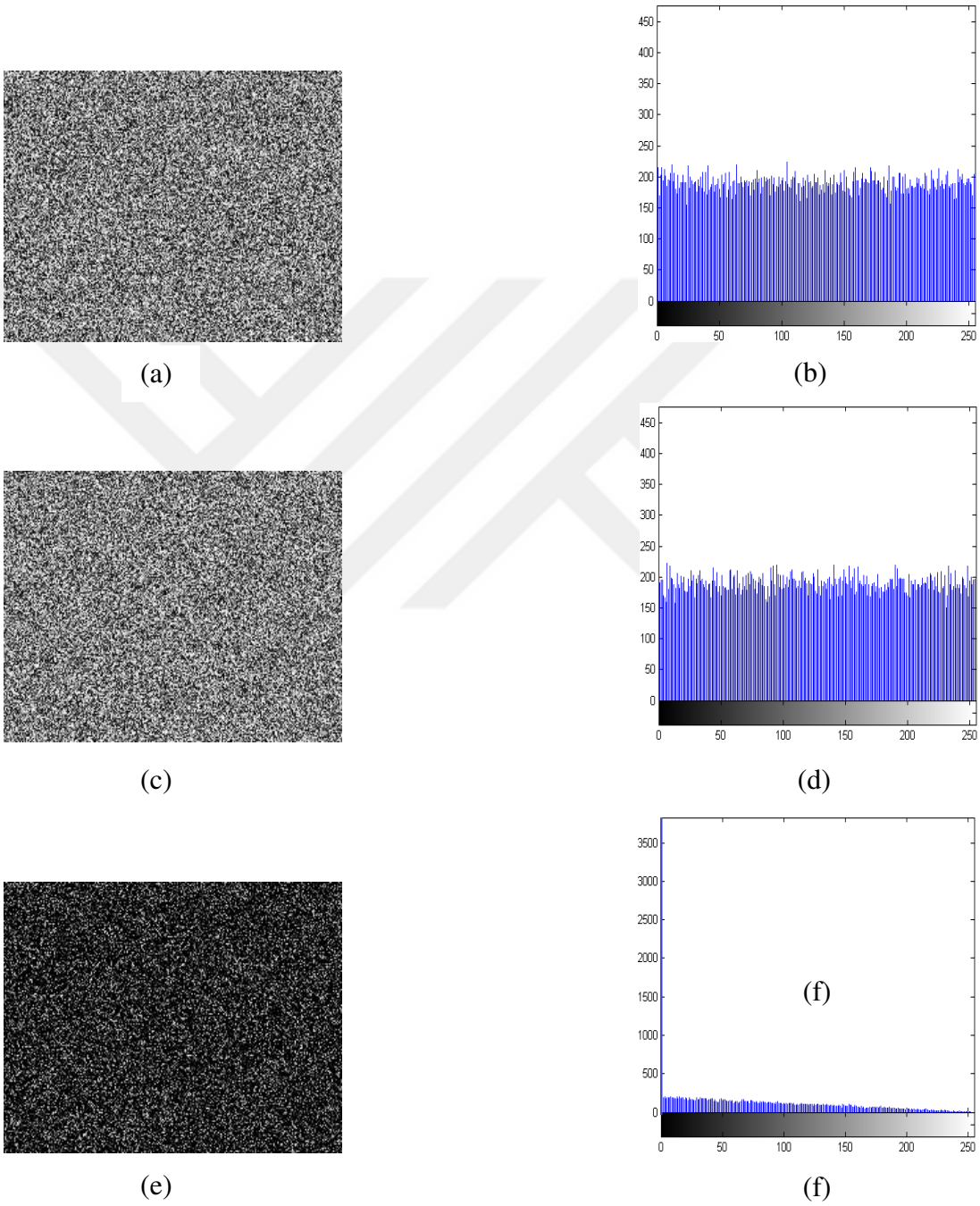
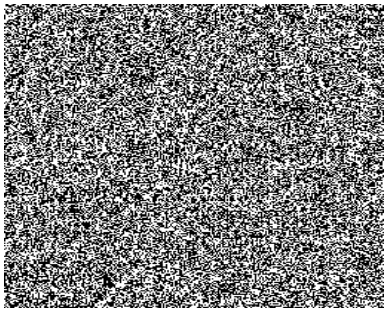
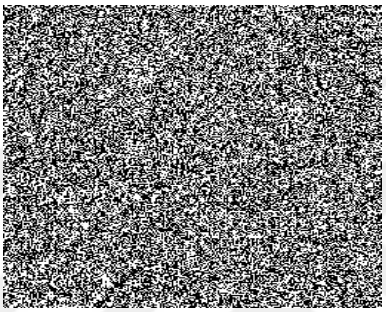


Figure 4. 4 Key sensitivity encryption plots for Barbara image: (a) encrypted with original keys; (b) corresponding histogram; (c) encrypted with changed keys; (d) corresponding histogram; (e) differential image; (f) corresponding histogram.

(a)



(b)



(c)

Figure 4. 5 Key sensitivity decryption plots for Barbara image: (a) decrypted with original keys; (b) decrypted with changed keys; (c) differential image.

is fairly sensitive to a tiny change in the keys and can withstand a differential attack efficiently.

5.3 Entropy Analysis

For a cryptosystem, its entropy value determines its strength against the entropy attack. Entropy basically measures how much the pixels in an image are randomly distributed. In other words, entropy quantifies the pixels distribution. For a random source with 256 emissions, the ideal entropy must be 8 [39]. Gray scale image has 256 different gray levels and each level have the same probability 1/256. Therefore, the ideal entropy can be calculated as [34]:

$$E.V = -\sum_{x=0}^{256-1} [P(x) \times log_2(P(x))] \tag{4.3}$$

$$= -\sum_{x=0}^{256-1} [\frac{1}{256} \times log_2(\frac{1}{256})]$$

$$= -\frac{1}{256} \times (\frac{1}{256}) \times log_2(\frac{1}{256})$$

$$= -log_2(\frac{1}{2^8})$$

$$= -log_2(2^{-8})$$

$$= -(-8) \times log_2(2)$$

$$= 8$$

For a good image encryption scheme, the entropy of the ciphertext image should be close enough to the ideal value 8. The computed values of entropy are shown in Table 4.2. The entropy values of plaintext and reconstructed images are not very close to the ideal one while the entropy values of ciphertexts are very close to the ideal value, which means that the ciphertexts have very good randomness as compared to plaintext original image and reconstructed image. Thus the proposed image compression and encryption scheme can strongly withstand the entropy attack.

Table 4. 2 Entropy values.

Image Type	Plaintext	Ciphertext	Rec-image
Barbara	7.6349	7.9968	7.7060
Boat	7.1251	7.9965	7.1736
Pepper	7.5942	7.9963	7.6313
Goldhill	7.4844	7.9955	7.5689

4.4 Robustness Analysis

4.4.1 Noise Attack

The ciphertext may be affected via noise during transmission. It is more difficult to recover an image from a ciphertext with noise. Therefore, an image encryption algorithm must be robust enough to resist noise attack in practical scenarios. To see the result of our designed image compression and encryption scheme in case of noise attack, the ciphertext generated via the proposed scheme is polluted with Salt and Pepper noise of density 0.2. Figure 4.6 illustrates the noise polluted ciphertext Barbara image and the reconstructed Barbara image. Thus one can conclude that the proposed image compression and encryption scheme is robust against noise attack.

4.4.2 Occlusion Attack

Sometimes the attacker tries to lose some data of the ciphertext image, which may affect the reconstruction of the original image greatly. This attack may change the

(a) (b)

Figure 4. 6 Noise robustness plots: (a) ciphertext image polluted with noise; (b) reconstructed image.

image content. Therefore, 50 x 50 pixels of the ciphertext image are cropped out to check the performance of the proposed image compression and encryption scheme in case of cropping attack. Figure 4.7 demonstrates the corrupted ciphertext Barbara image and the reconstructed Barbara image. It can be observed that the reconstructed image is distorted to some extent but the image is still understandable. Therefore, the proposed scheme is robust against occlusion attack.

(a) (b)

Figure 4. 7 Key sensitivity decryption plots for Barbara image: (a) decrypted with original keys; (b) decrypted with changed keys; (c) differential image.

4.5 Differential Attack Analysis

This analysis determines the ability of resistance of an image encryption scheme to differential attack in terms of sensitivity to plain text image. Standard Number of Pixel Changing Rate (NPCR) and Unified Average Changing Intensity (UACI) are generally used to compute the strength of resisting the differential attack. To analyze the sensitivity relationship of plaintext image and its corresponding ciphertext image, two ciphertext images E1 and E2 are generated via encrypting the original plaintext image and one pixel changed plaintext image, respectively. The rate of change in ciphertext image due to single pixel changed in the original image can be measured via NPCR while the average change intensity between plaintext image and corresponding ciphertext image can be computed via UACI. Mathematically NPCR and UACI can be calculated as [40]:

$$NPCR = \frac{\sum_{u,v} B(u,v)}{n \times m} \times 100. \tag{4.4}$$

$$UACI = \left(\frac{1}{n \times m}\right) \times [\sum_{u,v} \frac{|E_1(u,v) - E_2(u,v)|}{255}]. \tag{4.5}$$

Where

$$B(u,v) = \begin{cases} 0 & if \quad E_1(u,v) = E_2(u,v), \\ 1 & if \quad E_1(u,v) \neq E_2(u,v). \end{cases}$$

The computed values of NPCR and UACI for the presented image compression and encryption scheme are given in Table 4.3. Thus the higher values of NPCR and

UACI affirm that the proposed image compression and encryption scheme can resist the differential attack.

Table 4. 3 NPCR and UACI values.

Test	Barbara	Boat	Pepper	Goldhill
NPCR	99.6094%	99.6114%	99.5950%	99.6402%
UACI	33.3895%	33.3446%	33.4445%	33.4225%

4.6 Visual Strength Analysis

The strength of an image encryption scheme can be visualized via performing contrast, energy and homogeneity test. *u, v* and *P(u; v)* demonstrates pixel position and pixel value, respectively.

4.6.1 Contrast

Contrast analysis presents an object in the texture of an image and defines the variations in image pixels. Mathematically, contrast can be defined as [41]:

$$C = \sum_{u,v} |u - v|^2 P(u, v). \tag{4.6}$$

The computed values of the contrast test for the proposed image compression and encryption scheme are given in Table 4.4. The higher values of the contrast test for cipher image reveals that there is a large variation in cipher image pixels.

4.6.2 Energy

The energy test computes the disorderedness in the texture of the ciphertext image via summing the squared values in GLCM. Energy can be expressed as [41]:

$$Energy = \sum_{u,v} P(u, v)^2. \tag{4.7}$$

The calculated energy test values for the proposed image compression and encryption scheme are given in Table 4.4. The lower values of energy test for cipher image demonstrates that the encryption is of high quality.

4.6.2 Homogeneity

Homogeneity analysis defines the closeness of distribution in the Gray Level Co-occurrence Matrix (GLCM) to GLCM diagonal. Mathematically homogeneity can be calculated as [41]:

$$H = \sum_{u,v} \left(\frac{P(u,v)}{1 + |u - v|} \right). \tag{4.8}$$

The computed values of the homogeneity test for the proposed image compression and encryption scheme are given in Table 4.4. The lower values of the homogeneity test for cipher image reveals that there is a large variation in cipher image pixels.

Table 4. 4 Contrast, energy and homogeneity values.

Test	Image Type	Plaintext	Ciphertext	Rec-Image
Contrast	Barbara	1.0732	10.5164	1.1310
	Boat	0.2487	10.5120	0.2634
	Pepper	0.3301	10.5350	0.3377
	Goldhill	0.4445	10.5568	0.4915
Energy	Barbara	0.0635	0.0156	0.0563
	Boat	0.1977	0.0157	0.1900
	Pepper	0.1099	0.0245	0.1026
	Goldhill	0.1007	0.0159	0.0896
Homogeneity	Barbara	0.7692	0.3907	0.7450
	Boat	0.9096	0.3896	0.9017
	Pepper	0.8926	0.3889	0.8785
	Goldhill	0.8479	0.3887	0.8192

4.7 PSNR Analysis

In image processing, the quality of the reconstructed image can be judged via analyzing the Peak Signal to Noise Ratio (PSNR) of that particular image. Mathematically PSNR can be computed as [16]:

$$P.S.N.R = 10 \times log_{10} \left(\frac{(255 \times 255)}{M.S.E}\right). \tag{4.9}$$

$$M.S.E = \frac{\sum_{u=1}^{n} \sum_{v=1}^{n} (x(u,v) - x^*(u,v))^2}{n \times m}. \tag{4.10}$$

where MSE computes the mean variance of the plaintext and reconstructed images, *x(u, v)* and *x*(u, v)* represent pixels values of the plaintext and reconstructed images, respectively. The computed PSNR values for the proposed image compression and encryption scheme are illustrated in Table 4.5. The larger values of the PSNR (almost greater than 32 dB) reveals that the plaintext image and the reconstructed image are almost the same.

Table 4. 5 PSNR values.

Test	Barbara	Boat	Pepper	Goldhill
PSNR	32.0242	33.0012	32.2155	32.0057

4.8 Chosen-Plaintext and Know-plaintext Attacks Analysis

In this research work, the initial conditions for chaotic maps are computed via passing the plain image through *SHA-512* hash function. This dependency of initial conditions on the plaintext image makes the proposed image compression and encryption scheme secure against chosen-plaintext attack and known-plaintext attack. Thus, the production of all the random vectors and the measurement matrix are decided by the original plain image. In case, a single pixel change occurs in the plaintext image, the resultant key stream changes accordingly, and the generated ciphertext image will be a totally different one. If the eavesdropper tries to extract some useful information via encrypting some particular images, this plaintext dependency of the proposed scheme will always fail the eavesdropper. Therefore, the

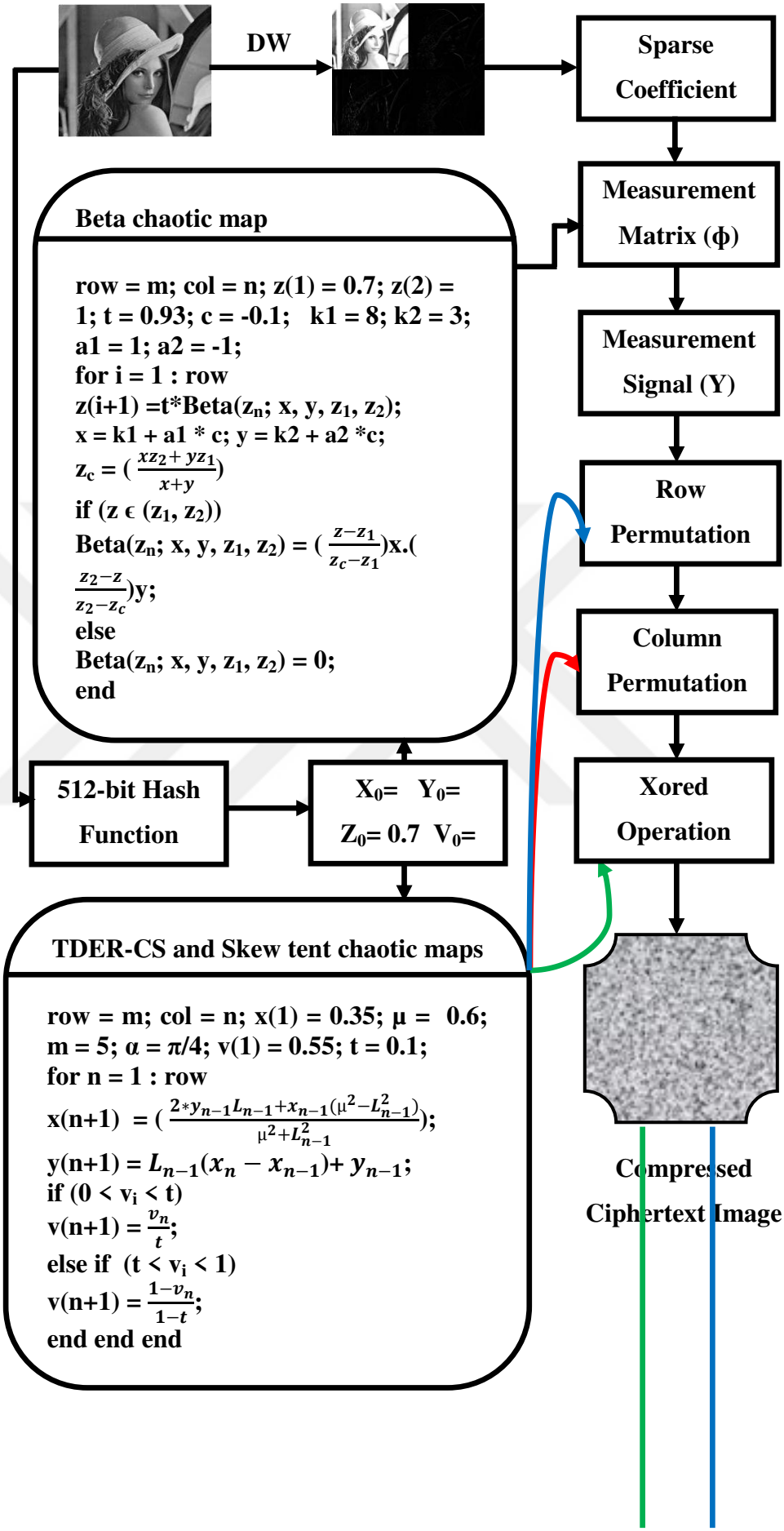
presented image compression and encryption scheme can withstand the chosen-plaintext and known-plaintext attacks.

CHAPTER 5
CONCLUSIONS AND FUTURE RESEARCH

In this paper, chaos and compressive sensing based novel image encryption scheme is investigated. Firstly, the original plaintext image is compressed via Orthogonal Matching Pursuit with Partially Known Support (OMP-PKS) greedy algorithm, which provides confidentiality and security using less number of data. Then the compressed image is confused and diffused using TD-ERCS and Skew-tent chaotic maps, respectively. For the sake of higher security, the initial conditions of chaotic maps are made dependent on the plaintext image and the parameters are computed via SHA-512. Furthermore, to decrease the transmission bandwidth and storage space, the measurement matrix is generated via Beta chaotic map.

The reliability and robustness of the designed image compression and encryption scheme are verified via statistical attack analysis, key analysis, entropy attack analysis, robustness analysis, visual strength analysis, PSNR, differential attack analysis, known-plaintext attack and chosen-plaintext attack analysis. All the experimental and simulation results reveal that the key space is large enough and the key is highly sensitive, the scheme can withstand noise, cropping, statistical, entropy, differential, know-plaintext, and chosen-plaintext attack efficiently and robustly.

The ciphertext image of many encryption schemes is a noise/texture-like image and thus resist various attacks i.e., known plaintext attack, chosen ciphertext attack etc. However, the possibility of attacks on noise like the image is very high. This problem can be overcome via designing visually secure image encryption scheme. Therefore, in future we can modifiy our designed “chaos and compressive sensing based novel image encryption scheme” to “chaos and compressive sensing based novel visually secure image encryption scheme”. The general flow diagram of the future visually secure image encryption scheme is demonstrated in Fig. [5.1].


DW
Sparse Coefficient
Measurement Matrix (ϕ)
Measurement Signal (Y)
Row Permutation
Column Permutation
Xored Operation
Compressed Ciphertext Image
Beta chaotic map
row = m; col = n; z(1) = 0.7; z(2) = 1; t = 0.93; c = -0.1; k1 = 8; k2 = 3;
a1 = 1; a2 = -1;
for i = 1 : row
z(i+1) =t*Beta(zn; x, y, z1, z2);
x = k1 + a1 * c; y = k2 + a2 *c;
zc = (xz2+ yz1 / x+y)
if (z ϵ (z1, z2))
Beta(zn; x, y, z1, z2) = (z−z1 / zc−z1)x.(z2−z / z2−zc)y;
else
Beta(zn; x, y, z1, z2) = 0;
end
512-bit Hash Function
X0= Y0= Z0= 0.7 V0=
TDER-CS and Skew tent chaotic maps
row = m; col = n; x(1) = 0.35; μ = 0.6;
m = 5; α = π/4; v(1) = 0.55; t = 0.1;
for n = 1 : row
x(n+1) = (2∗yn−1Ln−1+xn−1(μ2−Ln−12) / μ2+Ln−12);
y(n+1) = Ln−1(xn − xn−1)+ yn−1;
if (0 < vi < t)
v(n+1) = vn / t;
else if (t < vi < 1)
v(n+1) = 1−vn / 1−t;
end end end

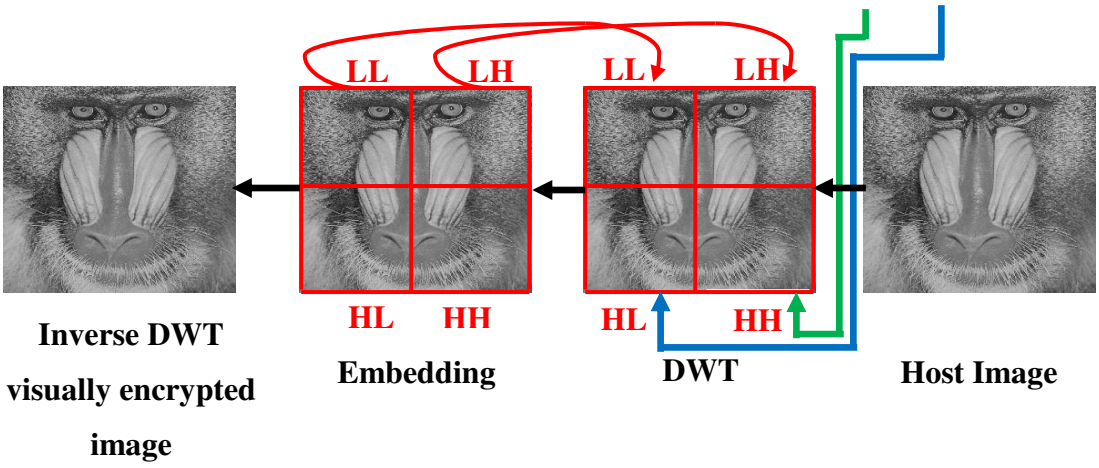


Figure 5. 1 Flow diagram of the future work.

REFERENCES

[1] Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code*. C John Wiley & Sons. Inc., America.

[2] Stallings, W. (2017). Cryptography and network security: principles and practice. *Upper Saddle River: Pearson*, **998**, 92-95.

[3] El-Ashry, I. E. (2010). Digital image encryption. MSc Thesis, Electronics and Electrical Communications Engineering Dept., Faculty of Electronic Engineering, Menofia University.

[4] Elminaam, D. S. A., Abdual-Kader, H. M., & Hadhoud, M. M. (2010). Evaluating the performance of symmetric encryption algorithms. *IJ Network Security*, **10(3)**, 216-222.

[5] Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos*, **16(08)**, 2129-2151.

[6] Matthews, R. (1989). On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, **13(1)**, 29-42.

[7] Liu, H., Kadir, A., & Gong, P. (2015). A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise. *Optics Communications*, **338**, 340-347.

[8] Ayoup, A. M., Hussein, A. H., & Attia, M. A. (2016). Efficient selective image encryption. *Multimedia tools and applications*, **75(24)**, 17171-17186.

[9] Khan, J. S., & Ahmad, J. (2018). Chaos based efficient selective image encryption. *Multidimensional Systems and Signal Processing*, 1-19.

[10] Wang, Y., Wong, K. W., Liao, X., & Chen, G. (2011). A new chaos-based fast image encryption algorithm. *Applied soft computing*, **11(1)**, 514-522.

[11] Zhang, Y., & Xiao, D. (2013). Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. *Optics and Lasers in Engineering*, **51(4)**, 472-480.

[12] Chai, X., Gan, Z., Chen, Y., & Zhang, Y. (2017). A visually secure image encryption scheme based on compressive sensing. *Signal Processing*, **134**, 35-51.

[13] Abbasi, S. F., Ahmad, J., Khan, J. S., Khan, M. A., & Sheikh, S. A. (2018, July). Visual Meaningful Encryption Scheme Using Intertwinning Logistic Map. *Science and Information Conference Springer, Cham*, 764-773.

[14] Xiao, D., Wang, L., Xiang, T., & Wang, Y. (2017). Multi-focus image fusion and robust encryption algorithm based on compressive sensing. *Optics & Laser Technology*, **91**, 212-225.

[15] Hu, G., Xiao, D., Wang, Y., & Xiang, T. (2017). An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications. *Journal of Visual Communication and Image Representation*, **44**, 116-127.

[16] Chai, X., Zheng, X., Gan, Z., Han, D., & Chen, Y. (2018). An image encryption algorithm based on chaotic system and compressive sensing. *Signal Processing*, **148**, 124-144.

[17] Khan, F. A., Ahmed, J., Khan, J. S., Ahmad, J., & Khan, M. A. (2017). A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S 8 permutation. *Journal of Intelligent & Fuzzy Systems*, **33(6)**, 3753-3765.

[18] Tawfic, I. S., & Kayhan, S. K. (2014). Least support orthogonal matching pursuit algorithm with prior information. *Journal of Applied Computer Science Methods*, **6(2)**, 111-134.

[19] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal*, **28(4)**, 656-715.

[20] Candes, E. J., & Romberg, J. (2006). Quantitative robust uncertainty principles and optimally sparse decompositions. *Foundations of Computational Mathematics*, **6(2),** 227-254.

[21] Candes, E. J., Romberg, J. K., & Tao, T. (2006). Stable signal recovery from incomplete and inaccurate measurements. Communications on Pure and Applied Mathematics: *A Journal Issued by the Courant Institute of Mathematical Sciences*, **59(8)**, 1207-1223.

[22] Donoho, D. L. (2006). Compressed sensing. *IEEE Transactions on information theory*, **52(4)**, 1289-1306.

[23] Aharon, M., Elad, M., & Bruckstein, A. (2006). K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation. *IEEE Transactions on signal processing*, **54(11),** 4311.

[24] Wright, J., Yang, A. Y., Ganesh, A., Sastry, S. S., & Ma, Y. (2009). Robust face recognition via sparse representation. *IEEE transactions on pattern analysis and machine intelligence*, **31(2),** 210-227.

[25] Zhang, Q., & Li, B. (2010, June). Discriminative K-SVD for dictionary learning in face recognition. *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2691-2698.

[26] Li, Y., Fermuller, C., Aloimonos, Y., & Ji, H. (2010, June). Learning shift-invariant sparse representation of actions. *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* 2630-2637.

[27] Patel, V. M., Easley, G. R., Healy Jr, D. M., & Chellappa, R. (2010). Compressed synthetic aperture radar. *IEEE Journal of selected topics in signal processing*, **4(2)**, 244-254.

[28] Tropp, J. A., & Gilbert, A. C. (2007). Signal recovery from random measurements via orthogonal matching pursuit. *IEEE Transactions on information theory*, **53(12)**, 4655-4666.

[29] Davenport, M. A., & Wakin, M. B. (2010). Analysis of orthogonal matching pursuit using the restricted isometry property. *IEEE Transactions on Information Theory*, **56(9)**, 4395-4401.

[30] Sermwuthisarn, P., Auethavekiat, S., & Patanavijit, V. (2009, January). A fast image recovery using compressive sensing technique with block based orthogonal matching pursuit. *2009 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, 212-215.

[31] Gibson, R. M., Amira, A., Ramzan, N., Casaseca-de-la-Higuera, P., & Pervez, Z. (2017). Matching pursuit-based compressive sensing in a wearable biomedical accelerometer fall diagnosis device. *Biomedical signal processing and control*, **33**, 96-108.

[32] Anselmi, N., Oliveri, G., Hannan, M. A., Salucci, M., & Massa, A. (2017). Color compressive sensing imaging of arbitrary-shaped scatterers. *IEEE Transactions on Microwave Theory and Techniques*, **65(6)**, 1986-1999.

[33] Ouyang, B., Hou, W. W., Caimi, F. M., Dalgleish, F. R., Vuorenkoski, A. K., & Gong, C. (2017). Integrating dynamic and distributed compressive sensing techniques to enhance image quality of the compressive line sensing system for unmanned aerial vehicles application. *Journal of Applied Remote Sensing*, **11(3)**, 032-407.

[34] Zahmoul, R., Ejbali, R., & Zaied, M. (2017). Image encryption based on new Beta chaotic maps. *Optics and Lasers in Engineering*, **96**, 39-49.

[35] Ke-Hui, S. L. Y. S., & Chuan-Bing, L. (2004). Study of a discrete chaotic system based on tangent-delay for elliptic reflecting cavity and its properties. *Acta Physica Sinica*, **9**, 011.

[36] Hasler, M., & Maistrenko, Y. L. (1997). An introduction to the synchronization of chaotic systems: Coupled skew tent maps. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, **44(10)**, 856-866.

[37] Khan, J. S., Khan, M. A., Ahmad, J., Hwang, S. O., & Ahmed, W. (2017). An improved image encryption scheme based on a non-linear chaotic algorithm and substitution boxes. *Informatica*, **28(4)**, 629-649.

[38] Khan, J. S., Ahmad, J., & Khan, M. A. (2017). Td-ercs map-based confusion and diffusion of autocorrelated data. *Nonlinear Dynamics*, **87(1)**, 93-107.

[39] Patro, K. A. K., & Acharya, B. (2019). An efficient colour image encryption scheme based on 1-D chaotic maps. *Journal of Information Security and Applications*, **46**, 23-41.

[40] Khan, F. A., Ahmed, J., Ahmad, J., Khan, J. S., & Stankovic, V. (2018, August). Intertwining and NCA Maps Based New Image Encryption Scheme. *2018 IEEE International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, 12-16.

[41] Waseem, H. M., & Khan, M. (2019). A new approach to digital content privacy using quantum spin and finite-state machine. *Applied Physics B*, **125(2)**, 27.