LOW BAND WIDTH HIGH SECURED IMAGE TRANSMISSION IN ROBUST CHANNELS

PAPPULA JAYASRILAKSHMI[2], SANTHI SRI RAYUDU[2]

[1]M.Tech Student, Dept. of ECE, Prasiddha College of Engineering & Technology, Anathavaram, AP
[2]Assistant Professor, Dept. of ECE, Prasiddha College of Engineering & Technology, Anathavaram, AP

ABSTRACT:- Privacy has always a growing impact on the modern applications and the growth in term of technology. The demand for the highest privacy must be guaranteed in the field of technical, commercial and legal regulations whenever sensitive information is stored, processed, or communicated in any form. Thus new technologies are also created new ways togather private information. In this system, to transmit data securely and to improve robustness, imperceptibility and payload capacity, combination of steganography and cryptography techniques are used. The referable values of secret image is embedded in the video file with the use of Arnold scrambling technique, discrete wavelet transformation and least significant bit. The secret key generated referable values of image is embedded behind the audio file. Before embedding of secret key, it is encrypted by a new proposed encryption algorithm, Twisted Exchange algorithm. Further, this project is enhanced by compressing secrete image to reduce bandwidth of the whole yield. So, computational time will be decreased to almost half to the former. Here, in this enhancement process HAAR wavelet transformation is used for reducing computational process.

INTRODUCTION:

Today images usually contain private or confidential information so that they should be protected from leakages during transmissions. Recently, many methods have been proposed for securing image transmission such as image encryption and data hiding. Image encryption is a technique that uses to encrypt image into noise form, using high redundancy and strong spatial correlation. The encrypted image is a meaningless file and before encryption additional information is not provided. Data hiding is alternative for image encryption that hide secret image into a cover image so that no one can realize the existence of the secret data. Large number of data is not hide into a single is the main issue of data hiding. Specifically, if one wants to hide a secret image into a cover image with the same size, the secret image must be highly compressed in advance. A new technique for secret image transmission is proposed with the help of secret image and target image. Select three images secret image, target image, and mosaic image. After selecting the target image, the given secret image is first divided into number of rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a comparison of colour transformation. Next, the color characteristic of each tile image is transformed into the other colour, resulting in a mosaic image which looks like the target image. Appropriate schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image [1].CURRENTLY, images from various sources are frequently utilized and transmitted through the internet for various applications, such as online personal photograph albums, confidential enterprise archives, document storage systems, medicalimaging systems, and military image databases. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Recently, many methods have been proposed for securing image transmission, for which two common approaches areimage encryption and data hiding. Image encryption is a technique that makes use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion and diffusion properties [1]–[7]

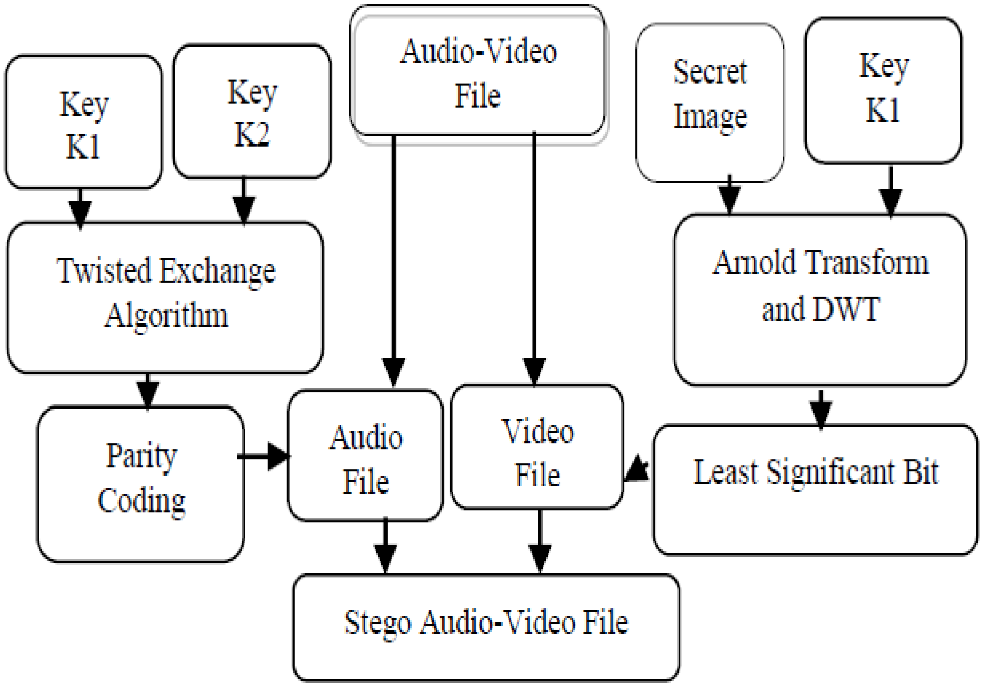


Fig: Transmitter block

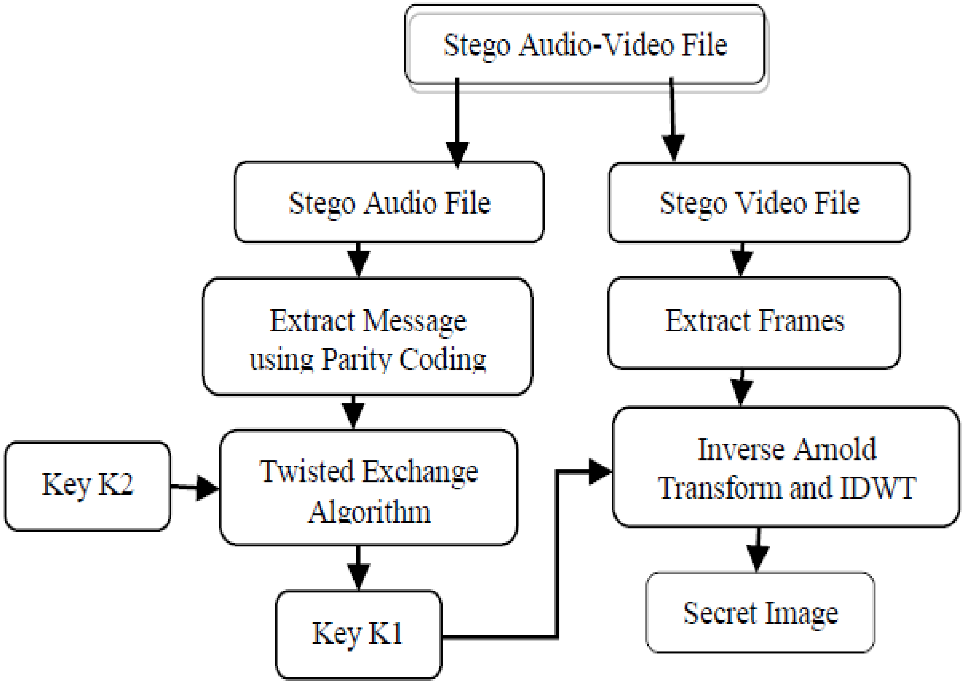

Stego Audio-Video File
Stego Audio File
Stego Video File
Extract Message using Parity Coding
Extract Frames
Key K2
Twisted Exchange Algorithm
Inverse Arnold Transform and IDWT
Key K1
Secret Image

Fig: Receiver block

This system combines both cryptography and steganography in order to provide higher level of security, imperceptibility, payload capacity, robustness. Moreover, to ensure the secret message (image) arrives to the intended receiver, double key encryption method is used. For the key encryption and decryption process, new proposed algorithm, Twisted Exchange algorithm is used. It provides fast communication speed and more secure system because it uses multiphase operations and its generated key streams are randomness and unpredictability. In the sender side of this system, it doesn't hide directly the secret message (image) into the cover video. Its partial referable values areembedded by using constant value and secret key. This secret key wants to hide behind the audio file, but, the key is not embedded directly because the intended receiver is provided more securely and correctly. Thus, the first secret key used for embedding of the secret message (image) is encrypted with the second secret key by using Twisted Exchange algorithm. Both sender and receiver must know the second secret key as a pre-shared key and the detail information of this system explains as the following two sides: sender side and receiver side.

A.ENCRYPTION PROCESSES (SENDER SIDE)

Fig.1 shows the embedding process of proposed system, in which the sender selects any one audio-video file and separates it into individual audio and video file which is a collection of multiple frames. Then the sender chooses a video file and a secret image which will be transmitted to the receiver. Before hiding the secret image behind the video file, it is scrambled by Arnold transform technique and the generated scrambled image is decomposed as approximation and details values by discrete wavelet transform (DWT)[8][9]. Referable values obtained from frequency values are embedded into red, green and blue (RGB) channel of the selected frame by applying least significant bit (4LSB) technique. Referable values aregenerated by using secret key (key K1) and constant values. These are shown in the following three equations: (1), (2) and (3). After embedding the secret image behind the video frames, the stego frames and the other remained frames are reassembled to stego video file. In order to provide higher level of security for the system, double key encryption method is used. It means that the first secret key (key K1) used for embedding the secret message (image) is encrypted with the second secret key (key K2) by Twisted Exchange algorithm. Then, the received encrypted message and selected frame number are hided into the audio file using parity coding algorithm [10] as stego audio file. Finally, the received stego video file and stego audio file are combi into one stego audio-video file and send this stego file to the receiver through the internet.

$B = \text{floor}\ (F/S)$ (1)

$R = \text{floor}\ (\text{mod}\ (F, S)/k)$ (2)

$G = \text{mod}\ (\text{mod}\ (F, S), k)$ (3)

where, R, G and B are three color channels of the frame. F is frequency values of the secret message (image), S is secret key and k is constant value.

DECRYPTION PROCESSES (RECEIVER SIDE):

In the extraction processes (receiver side), receive selects the stego audio-video file and it is separated again into individual stego audio and stego video file. To retrieve the secret message (image) sent from the sender, firstly the receiver must choose stego audio file and extract the message and frame number in it by using parity coding technique. And, the message is decrypted with secret key (key K2) that is known both the sender and receiver by using Twisted Exchange algorithm. Then the resulted decrypted message that means the secret key to extract the secret message (image) embedded in the stego video file is used. Referable values are extracted from the selected frame number and these values convert to original frequency values . With the use of inverse Discrete Wavelet Transform (IDWT)and inverse Arnold scrambling technique, the original secret message (image) is rebuild from frequency values. As this way the secret image is received securely and secretly by the receiver.

TWISTED EXCHANGE ALGORITHM:

The combination of steganography and cryptography provides a more secure system. Therefore, in this system this hybrid method is used. In the part of cryptography, new proposed encryption algorithm, Twisted Exchange algorithm is used. It is based on stream cipher model and used type of pseudorandom number generator. Thus, the processing speed of this algorithm is fast. On the other way, the life of stream cipher is key generation step. If the keys stream generated from the key generation step is nonrandom, an unauthorized user or intruder can predict or analyse the secret message. So, the keys stream generation must be random because it is important and necessary that everyone except the user don't know about it. Thus, the proposed algorithm consists of random exchange and multiphase operation to provide random key stream. In this system, the algorithm is used to encrypt and decrypt the user's secret key (key K1) with second key (key K2), presharedkey that is known both sender and receiver. According to the stream cipher rule, the second secret key (key K2) is converted into the initial seed value that means as the input of pseudorandom number generator. The algorithm calculates the initial seed value by the following equation.

$$seed = \sum_{i=1}^{n} ASCII(xi) * i$$

And the length of a key stream generated by pseudorandom number generator is equal to the length of plain (cipher) text. Finally, the result key stream and plain (cipher) text are operated with XOR to produce the cipher (plain) text. Encryption and decryption of Twisted Exchange algorithm is expressed in below.

Step 1: Convert ASCII values of plain (cipher) text and secret key, and generate a seed from the secret key.

Step 2: Generate random key stream as long as plain (cipher) text by using pseudorandom number generator. The following steps are executed repeatedly as long as the length of plain (cipher) text Firstly, calculate the three new values from the seed by using subtracting, multiplication and modulation with a number 256. Execute exclusive-OR operation with the seed and above one of the three values. Exchange random two pair bits and then execute again exclusive-OR operation, modulation subtraction until all of these operations are performed repeatedly four times. Operate exclusive-OR operation of the above value with one of the three values. Generate a random key by using addition and modulation with a number, and next seed value is obtained by adding of random key.

Step 3: Produce cipher (plain) text by using exclusive-OR operation with generated key stream and plain (cipher) text. Execute exclusive-OR operation of plain (cipher) text with generated key stream. According to the most significant bit (MSB) of the above result, do again exclusive-OR operation with the result and 255 or zero.

ARNOLD TRANSFORM:

A digital image can be considered as a two unit function f(x,y) in the plane Z. It can be represented as Z = f(x,y) where x,y ∈{0,1,2,3....N-1} . Hence, N represents order of digital image. The matrix of image can be changed into a new matrix by using the Arnold transform which results in a scrambled version to offer better security. It is a mapping function which changes a point (x,y) to another point (x′ , y′)

X'=(x+y) mod N

Y'=(x+2y) mod N

The Arnold transform is a classical 2D invertible chaotic map defined as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 \qquad 1$$

The inverse transform is defined as:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod 1 \qquad 2$$

IMAGE COMPRESSION:

Image compression addresses the problem of reducing the amount of data required to represent a digital image [5,6]. It is a process intended to yield a compact representation of an image, thereby reducing the image storage/transmission requirements. Compression is achieved by the removal of one or more of the three basic data redundancies i.e Coding redundancy, Interpixel redundancy and Psychovisual redundancy.

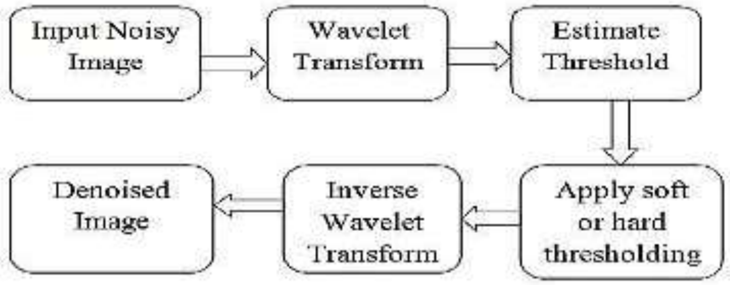
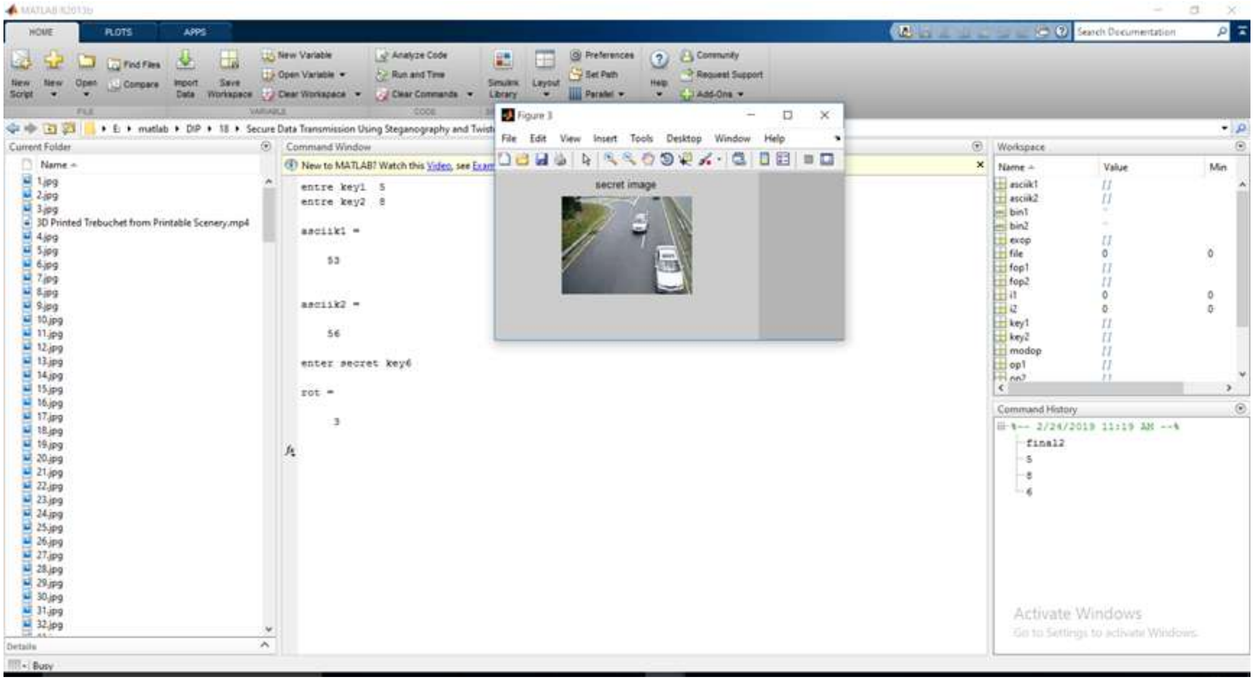


Figure: Basic Steps in image compression system

The main drawback of the DWT is that the wavelet coefficients are real numbers. In this case efficient lossless coding is not possible using linear transforms. The lifting scheme (LS) presented by Sweldens allows an efficient implementation of the DWT. Another of its properties is that perfect reconstruction is ensured by the structure of the LS itself. This allows new transformations to be used. One such transformation is the Integer wavelet transform (IWT) [7] it is a basic modification of linear transforms, where each filter output is rounded to the nearest integer. IWT can be used to have a unified lossy and lossless codec. It is also of interest for hardware implementations, where the use of floating point is still a costly operation. The wavelet Lifting Scheme is a method for decomposing wavelet transforms into a set of stages. The convolution-based 1-D DWT requires both a large number of arithmetic computations and a large memory for storage. Such features are not desirable for either high speed or low power image processing applications. The main feature of the lifting-based wavelet transform is to break-up the high pass and the low pass wavelet filters into a sequence of smaller filters [8]. The lifting scheme requires fewer computations compared to the convolution-based DWT. Therefore the computational complexity is reduced to almost a half of those needed with a convolution approach.

RESULT:



E: ▸ matlab ▸ DIP ▸ 18 ▸ Secure Data Transmission Using Steganography and Twist

Current Folder

Name
1.jpg
2.jpg
3.jpg
3D Printed Trebuchet from Printable Scenery.mp4
4.jpg
5.jpg
6.jpg
7.jpg
8.jpg
9.jpg
10.jpg
11.jpg
12.jpg
13.jpg
14.jpg
15.jpg
16.jpg
17.jpg
18.jpg
19.jpg
20.jpg
21.jpg
22.jpg
23.jpg
24.jpg
25.jpg
26.jpg
27.jpg
28.jpg
29.jpg
30.jpg
31.jpg
32.jpg

Command Window

New to MATLAB? Watch this Video, see Exam

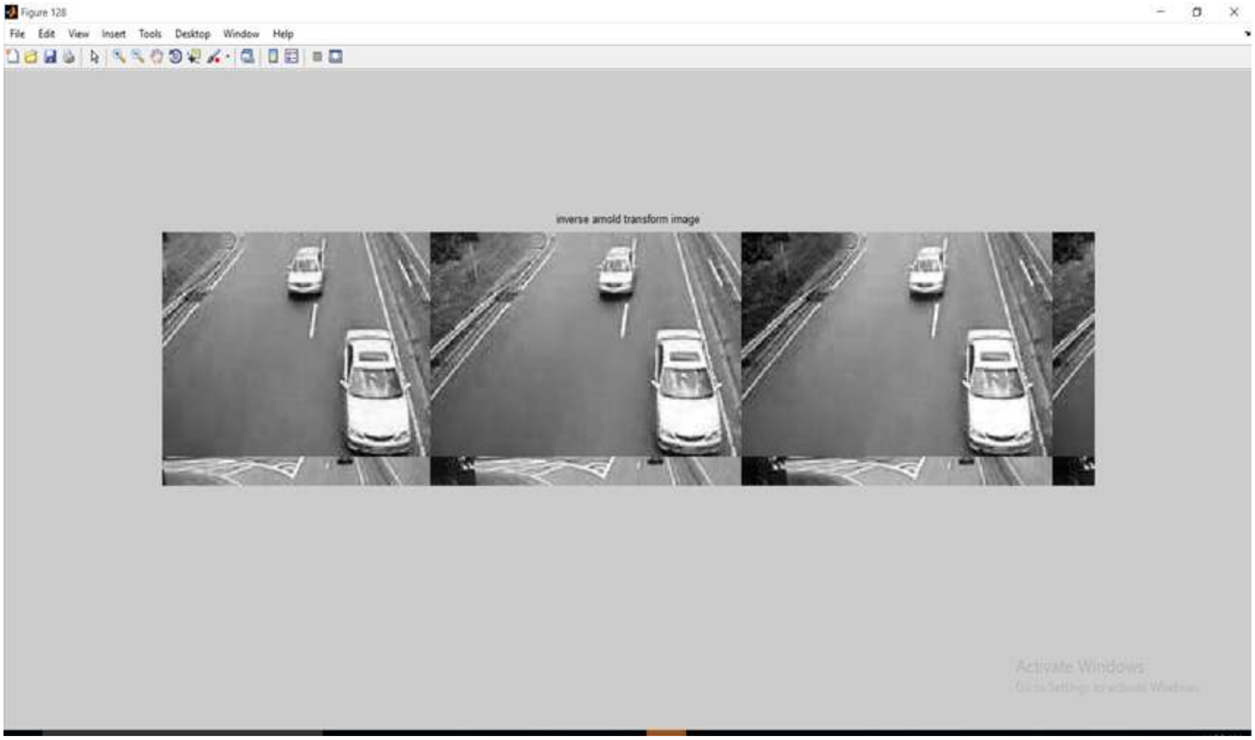
```
entre key1  5
entre key2  8

asciik1 =

    53


asciik2 =

    56

enter secret key6

rot =

     3
```

Workspace

Name	Value	Min
asciik1	[]	
asciik2	[]	
bin1	''	
bin2	''	
exop	[]	
file	0	0
fop1	[]	
fop2	[]	
i1	0	0
i2	0	0
key1	[]	
key2	[]	
modop	[]	
op1	[]	
op2	[]	

Command History

```
%-- 2/24/2019 11:19 AM --%
  final2
  5
  8
  6
```



CONCLUSION:

This paper presented a steganographic method to combine data hiding and encryption of digital images. Only the genuine receivers with access to the shared key can extract both the message and the original cover image. The image is recovered with minimal losses. Arnold Mapping is used to ensure that the image pixels are thoroughly scrambled and the random diffusion step overcomes the limited period of the mapping. Thus the cryptographic security is enhanced. Experimental results demonstrate the effectiveness of the proposed method. Future efforts can be made to increase the embedding capacity.

REFERENCES

[1] J. Kim and F. Pellacini, "Jigsaw image mosaics," Proc. of 2002 Int'l Conf. on Computer Graphics &Interactive Techniques (SIGGRAPH 02), San Antonio, USA, July 2002, pp. 657-664.

[2] Y. Dobashi, T. Haga, H. Johan and T. Nishita, "A method for creating mosaic image using voronoidiagrams," Proc. of 2002 European Association for Computer Graphics (Eurographics 02), Saarbrucken, Germany, Sept. 2002, pp. 341-348.

[3] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst.Video Technol*., Vol. 13, No. 8, Aug. 2003, pp. 890– 896.

[4] Ming-Shing Su, Wen-Liang Hwang, and Kuo-Young Cheng "Analysis on Multi resolution Mosaic Images"*IEEE transactions on image processing*, Vol. 13, No.7, July 2004, pp. 952-959.

[5] Lukac and Plataniotis "digital image indexing using secret sharing schemes: a unified framework for single-sensor consumer electronics" *IEEEtransactions on consumer electronics*, Vol. 51, No. 3, August 2005, pp. 908-917.

[6] S. Battiato, G. Di Blasi, G.M. Farinella and G. Gallo, "Digital mosaic framework: an overview," Euro graphics – Computer Graphic Forum, Vol. 26, No. 4, Dec. 2007, pp. 794-812.

[7] I. J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic image A new computer art and its applicationto information hiding," *IEEE Trans. Inf. Forens. Secure*, Vol. 6, No. 3, Sep. 2011, pp. 936–945.

[8] LI Jing “Remote Viewing Image Mosaic based onFuzzy Cellular Automata Corner Detection in Substation” *International Journal of Security and Its Applications* Vol.7, No.6 (2013), pp.55-66.

[9] Hae-Yeoun Lee “Generation of Photo-Mosaic Images through Block Matching and Color Adjustment *“International Journal of Computer, Information, Systems and Control Engineering* Vol.: 8 No:3, 2014, pp. 426-430.

[10] Ya-lin lee and Tsai *IEEE transactions on circuits and systems for video technology*, Vol. 24, No. 4, April 2014, pp. 695-704.

[11] Y. Hu, H.-K. Lee, K. Chen, and J. Li, “Difference expansion based reversible data hiding using two embedding directions,” *IEEE Trans. Multimedia*, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.

[12] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” *IEEE Trans. Circuits Syst. Video Technol*., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[13] X. Li, B. Yang, and T. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[14] W. Zhang, X. Hu, X. Li, and N. Yu, “Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression,” *IEEE Trans. Image Process.*, vol. 22, no. 7, pp. 2775–2785, Jul. 2013.