A Secure and High-Capacity Data-Hiding Method using Arnold Transform and Chaotic Scrambling

K.B Loganathan[1], M Kishor[2], C Muniyappan[3], Dr.S Karthigai Lakshmi[4]

[1,2,3]Under Graduate student, ECE Department, SSMIET, Dindigul, Tamil Nadu, India
[4]Associate Professor, ECE Department, SSMIET, Dindigul, Tamil Nadu, India

---***---

Abstract: *In the fast growing digital world, the protection and transmission of data securely is becoming huge challenge through an open medium like internet. There are several methods for information security process like Cryptography and Steganography. The different data hiding method are lossless compression, advanced encryption standard (AES), modified pixel value differencing (MPVD), and least significant bit (LSB) substitution is presented. In the lossless compression, Arithmetic coding was applied on a secret message to provide 22% higher embedding capacity. The hidden message which is compressed is then given to AES encryption for better security. After compression and encryption, the LSB substitution and MPVD are applied in this work. The proposed scheme is composed of Arnold scrambling and chaotic scrambling (SC-HAC).The security is considered by the proposed scheme which combines Arnold scrambling and Logistic scrambling to improve the encryption effect. Here, Arnold transform and chaotic scrambling is used to increase the SSIM value for better quality of compressed image.*

Keywords: Arnold Transform, chaotic scrambling, encryption, decryption, cover image, Digital Image Processing, Steganography, chaos, Reversible data hiding, absolute moment block truncation coding (AMBTC).

1. INTRODUCTION

Steganography is method of hiding information in which prevent the detection of hidden messages and this can be achieved by hiding information inside another piece of innocent looking information. The different embedding methods are the spatial, time domain methods, Transform domain methods, etc. These methods hide/embed information in numerous kinds of media like text, image, audio, video etc. Among these types of different file formats, digital images are considered to be the foremost popular style of carriers due to their size and distribution frequency. Covert or hidden communication is that the process of hiding data in another information. There are many hidden communication techniques such as, Cryptography, Steganography, Covert channel, Watermarking etc. Steganography is the effective means of information or data hiding that protects information from unauthorized disclosure. It works by hiding secretive information into ordinary and innocent looking messages those are generally out of suspicion.

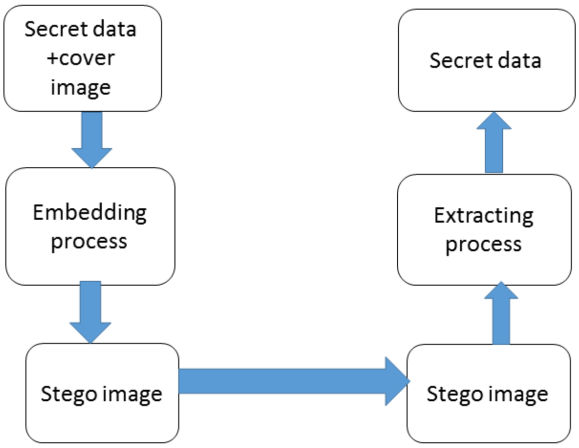


Fig.1 General Structure

The proposed system has following methods; they are embedding phase and the extraction phase. Within the embedding phase, the secretive message is first scrambled using transform at different levels, to create it safer against unauthorized extraction. This scrambled message is embedded into the cover image to get the stego image .then the stego image is transmitted and at the receiving end the hidden secret message is extracted by following the extraction and decryption process within the reverse order. During this technique, the values are kept secret and are only known to the authorized users and extraction without the keys results with noises, making the procedure secure.

2. STATISTICAL ELEMENTS

2.1 Mean:

Mean value gives the contribution of each pixel intensity for the whole image & variance is normally used to find how every pixel varies from the nearby pixel .The mean gives an idea where your pixels are (i.e. are they black, white, 50% gray,). The mean will give you an idea of what pixel color to choose to summarize the color of the complete image

2.2 Standard deviation:

Standard deviation is a numerical concept used to tell how measurements for a group are spread out from the average (Mean), or expected value. A low standard deviation means that most of the numbers are more close to the average. A high standard deviation means that the numbers are wide spread out. It is a mostly used to measure of variability or diversity used in statistics. A low standard deviation (LSD) indicates that the data points tend to be very close to the average (mean), whereas high standard deviation indicates that the data points are spread out over a large range of values. A standard deviation assigns value to the center pixel in the output map

2.3 SSIM:

The Structural Similarity Index (SSIM) is a perceptual metric that quantifies image quality reduction caused by processing such as data compression or by losses in data transmission.

The advantage of the SSIM metric is that it better represents human visual perception than does PSNR. SSIM is more complex, however, and takes more time to calculate and it is efficient..

Mat lab calculation for SSIM
[1]. ssimval = ssim (A, ref) computes the structural similarity (SSIM) index for grayscale image or volume A using ref as the reference image.

[2]. [ssimval, ssimmap] = ssim (A, ref) also returns the local SSIM value for each pixel in A.

2.4 PSNR:

Peak signal-to-noise ratio (PSNR) is the ratio between the highest possible power of an image and the power of some corrupting noise that affects the quality of its representation. To estimate the PSNR of an image, it is necessary to evaluate that image to an ideal clean image with the maximum possible power also returns the local SSIM value for each pixel in V

[ssimval, ssimmap] = ssim(V, reference)

3. PROPOSED SYSTEM AND DEVELOPMENT

3.1 Arnold Transform:

It is applied to a digital image randomizes the actual organization of its pixels and also the image becomes imperceptible or noisy. The matrix of image are often become a replacement matrix by using the Arnold transform which ends during a scrambled version to supply better security.

The transformation of point (x, y) within the unit square change to a different point (X ', Y ') is

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \pmod 1$$

3.2 Security Improvement by Chaotic Encryption:

The safety of the data-embedded AMBTC images is further enhanced using the proposed chaotic encryption method. Chaotic mapping is non-periodic and unpredictable. Thus, disrupting the characteristics of the image by chaotic mapping is appropriate, and the chaotic sequences are suitable for image encryption. To confuse the data-embedded image, the image of size M × N is reshaped into a one-dimensional sequence Ei,i = 1,2,...,M × N. To create chaotic behavior, the following chaotic equations are selected:

1) chaos logistic equation

xL n+1 = μ1xL n (1 − xL n),…… (1) And,

2) Chaos sine equation

xS n+1 = μ2sin(πxS n), …………(2)

If μ1 = 3.9 and μ2 = 0.89.

The above equations are obtained by setting x0 as 0.1 in (1) and (2), respectively. Mapping position is obtained by, two mapping sequences (EL i and ES i) are generated by rearranging the chaotic sequences as:

EL i = sort (unique (xL i))... (3) and

ES i= sort (unique (xS i))… (4)

where unique indicates a delete function which deletes repetitive elements of the sequences, and sort indicates a sorting function which sorts the sequence by size and records the rearrangement.

Finally, a Boolean XOR operator is used to diffuse the pixels as follows:

Ci = PL i⨁ rescale (xS i), if i ∈ even

PS i⨁ rescale (xL i), if i ∈ odd….(5)

Where rescale indicates a normalized function which scales xL i (and xS i) into an integer sequence within the interval of [0, 255], and Ci indicates the pixels of a cipher image in a one-dimensional sequence. The decryption system is based on the inverse process of the above encryption algorithm.

3.3 Block Diagram

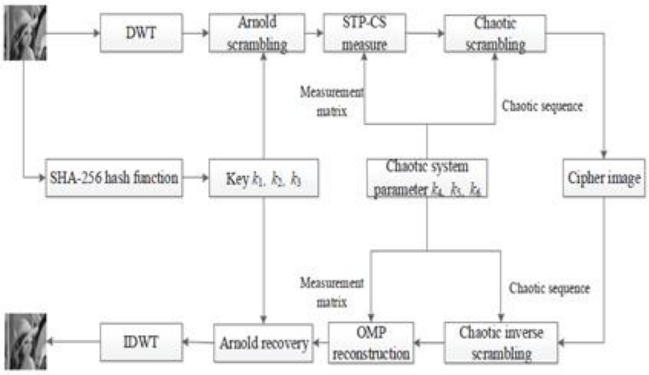


FIG.2 Block of proposed scheme SC-HAC.

The encryption process is presented as follows:

Step 1: According to the plain image *P*1, the keys *k*1, *k*2 and *k*3 can be calculated.

Step 2: The plain image is *P*1, whose size is $p \times q$. The discrete wavelet transform (DWT) is performed to get *P*2, whose size is still the same as that of *P*1. DWT can only be performed on a square matrix.

Step 3: Arnold scrambling is performed on *P*2 to get *P*3 whose size is $p \times q$. The parameters are *k*1, *k*2, *k*3, where *k*1 is Arnold scrambling number, and *k*2 and *k*3 are Arnold scrambling parameters.

Step 4: *P*3 is considered as *x*. performing a semi-tensor compressive sensing measurement, *y* can be obtained. *y* is denoted as *P*4 whose size is $mp=n \times q$, and *P*4 is the result of compression and encryption. In the model of $y = \alpha\emptyset1$ n
$x + \beta\emptyset2$, when $n \not= p$, ∅1, *x* can be calculated because we use semi-tensor compressive sensing. We take $n < p$ in the simulation experiments.

Step 5: Logistic chaotic scrambling is an application of Logistic chaotic system. First, we get the Logistic chaotic sequence *w* according to specific chaotic parameters. Then, we put the sequence *w* in ascending order to get the sequence *v*. The position of each element in the sequence *v* appearing in the original sequence *w* is denoted as the index sequence v. That is, $\emptyset(j) = i$ for $v(j) = w(i)$, where $i; j$ are integers and $1 \leq i; j \leq mp=n \times q$. Finally, according to the index Sequence, we scramble *P*4 to get the final cipher image *P*5 with size $mp=n \times q$. That is, $P5(k') = P4(\_(k'))$, where k' $(1 \leq k' \leq mp=n \times q)$ is the index. In the generation process of Logistic chaotic sequence, the control parameter is 4, and the chaotic initial value is *k*6. The initial sampling position is 1, and the sampling interval is 4.

4. EXPERIMENTAL RESULTS AND ANALYSIS

4.1 Encryption Results

The encryption result include the input image, Gray image, Embedded Input image and Embedded output image and the statistical parameter metrics are calculated for the images are Mean, Standard Deviation, SSIM, MS-SSIM.

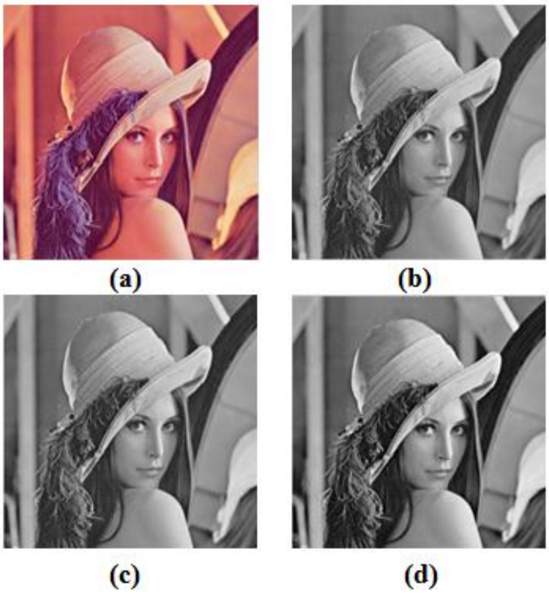
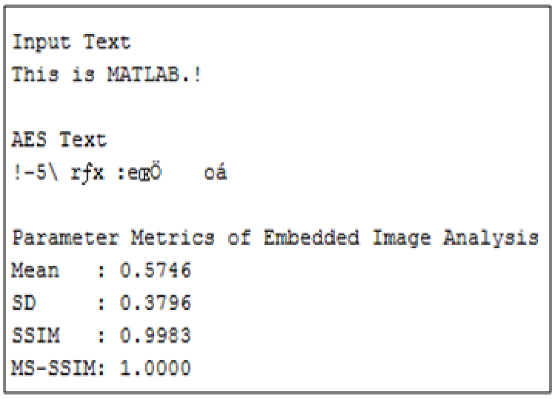


Fig.3 (a) Input image, (b Gray image, (c) Embedded Input image, (d) Embedded output image



```
Input Text
This is MATLAB.!

AES Text
!-5\ rƒx :eɶÖ    oá

Parameter Metrics of Embedded Image Analysis
Mean   : 0.5746
SD     : 0.3796
SSIM   : 0.9983
MS-SSIM: 1.0000
```

Table.1 Encryption with parameter metrics

4.2 Decryption Results:

The decryption result include the Extraction Input image and Extraction Output Image and the statistical parameter metrics are calculated for the images are Mean, Standard Deviation, SSIM, MS-SSIM.

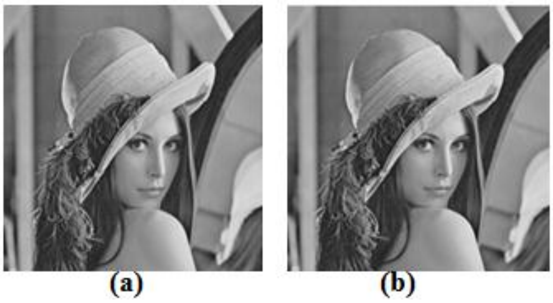
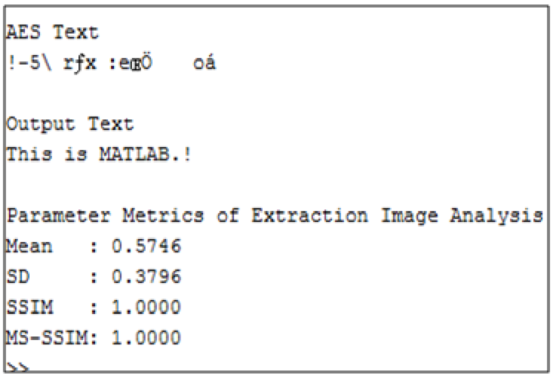


Fig.4 (a) Extraction Input image, (b) Extraction Output Image



```
AES Text
!-5\ rfx :e□Ö    oá

Output Text
This is MATLAB.!

Parameter Metrics of Extraction Image Analysis
Mean   : 0.5746
SD     : 0.3796
SSIM   : 1.0000
MS-SSIM: 1.0000
>>
```

Table.2 Decryption with parameter metrics

5. CONCLUSION

The secure and high capacity image steganography method is proposed and arithmetic coding is used for high embedding capacity, AES for additional security of hidden contents; MPVD, LSB and pixel optimization for enhanced capacity and improved visual quality. An enhanced embedding capacity of 3% more than earlier methods has been achieved using MPVD. MPVD and arithmetic coding together resulted in 25% higher embedding capacity. Through Arnold transform and chaotic scrambling the SSIM value for better quality of compressed image is achieved. Thus, proposed scheme promises significant advancement over existing methods.

6. ACKNOWLEDGEMENTS

First and foremost, we would like to express our deep sense of gratitude to our most honorable Chairman and Management Trustee Mr.P.S.Velusamy, our honorable secretary and Management Trustee Mr.C.Kandaswamy, our beloved Executive Directors and Management Trustee Mr.K.Shanmugavel and Mr.K.Sivaraj of SSM Institute of Engineering and Technology for providing us with necessary facilities during the course of study.
We feel immensely pleased to express our sincere thanks to our Principal Dr.D.Senthil kumaran for encouragement and support extended by them.

We extend our solemn gratitude to Dr.S.Karthigai Lakshmi, Head of the Department, Electronics and Communication Engineering, for her timely support to all our activities.

REFERENCES:

[1]Junhui He, Shuhao Huang, Shaohua Tang, Member, IEEE, Jiwu Huang, “JPEG Image Encryption with Improved Format Compatibility and File Size Preservation” submitted to IEEE transactions on multimedia, 2018

[2]Hsiang-ying wang, Hsin-ju lin, xiang-yun gao, Wen-huang cheng and yung-yao chen , “Reversible AMBTC-Based Data Hiding With Security Improvement by Chaotic Encryption” April 5, 2019.

[3]P. Rahmani and G. Dastghaibyfard, ‘‘Two reversible data hiding schemes for VQ-compressed images based on index coding,’’ IET Image Process, Jul. 2018.

[4]D. Xu, R. Wang, and Y. Shi, “An improved scheme for data hiding in encrypted H.264/AVC videos,” J. Vis. Commune. Image Represent. Apr. 2016.

[5]C.-N. Yanga,S.-C. Hsua, and C. Kim, “Improving stego image quality in image interpolation based data hiding” Comput. Standards Interfaces, Feb. 2017.