Enhancement of Image Security with New Methods of Cryptography and Steganography

Mani Bharathi. V[1], Manimegalai. M[2], Sinduja. V[3] [1,2,3] Department of Electronics and Communication Enginering,
P. A. College of Engineering and Technology, Pollachi, Tamil Nadu, India.

***Abstract*—In recent years, one of the necessary requirements of communication is to prevent data theft and securing the information. Security has become a critical feature for thriving networks and in military alike. Encryption technology has been developed quickly and many image encryption methods have been put forward. Chaos based image encryption technique is a new encryption technique for images. This paper introduces steganography involving Chaos Algorithm to encrypt the data as well as to hide the encrypted data in another medium, so the fact that a message being sent is concealed, is introduced.**

***Keywords* — Muddle, Chaos Algorithm, Steganography, Cryptography.**

I. INTRODUCTION

Cryptography (from Greek kryptós, "hidden", and gráphein, "to write") is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge, the art of encryption. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages no-matter how unbreakable will arouse suspicion. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Image encryption algorithm based on Chaotic Algorithm shows advantages of large key space and high-level security, while maintaining acceptable efficiency. Compared with some general encryption algorithms such as DES, the encryption algorithm is more secure. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications.

II. ANALYSIS OF ALGORITHMS

The thought of image encryption which combining the chaos with conventions is not only innovative but also feasible. Usage of Chaos Algorithm inevitably leads to many advantages:

1) Chaos in nature is multidisciplinary which broadly covers physics, mathematics, communications, engineering and so on. The first notion of applying chaos to encryption appeared in Shannon's famous paper of cryptography in 1949. As the principle of contemporary cryptographic design, he pointed out that: "In a good mixing transformation … functions are complicated, involving all variables in a sensitive way. A small variation of any one (variable) changes (all the outputs) considerably." This refers to the concept of confusion and diffusion, which can be connected to the fundamental properties of chaotic systems such as ergodic and sensitivity to initial conditions.

2) Encryption using the Chaos has a very good solution for high degree of redundancy issues. The problem of slow speed environment is also eliminated. For example, in the same environment, chaotic algorithms need 14 seconds to encrypt 500 K of the image data, while the DES needs 467 seconds.

3) Some important properties characterized by chaotic maps include sensitive dependence on initial conditions, sensitive dependence on system parameters and mixing in phase space.

III. PRINCIPLES OF ENCRYPTION

According to the idea of the literature, the principles of encryption algorithm have the following steps:

Step 1: Separation of RGB planes of the Message Image.
Step 2: Divide each plane into six blocks randomly and perform Arnold's Cat Map. This process is known by 'Random Strategy Arnold's Cat Map'.
Step 3: Get the Key Images and perform Chaos Encryption for the Message Image using the key features.
Step 4: Perform Steganography that is, hiding the encrypted Message Image behind the Cover Image. The resulting image is Stego Image.

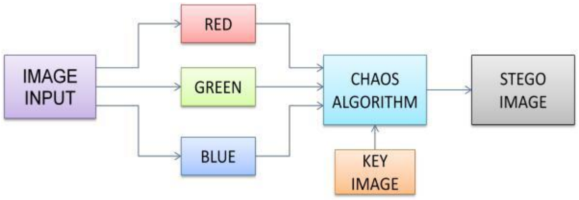


Figure 1. Principle of Encryption

A. *Plane Separation*

The digital color image consists of primary color planes, namely red, green and blue. These color planes cannot be processed together, hence there arises the need of *plane separation*. The three color planes are apportioned and are processed independently. Figure 2, shows the digital image of message image and its three planes.

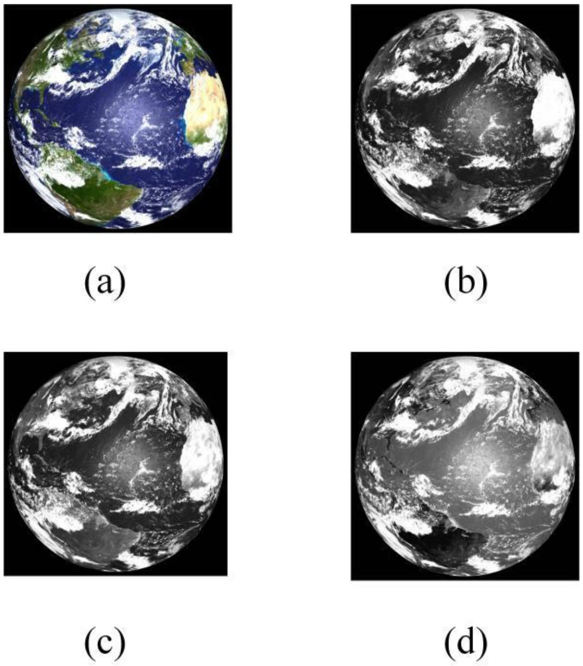


Figure 2. (a) Message Image, (b)RED Plane of Message Image, (c) GREEN Plane of Message Image, (d) BLUE Plane of Message Image.

B. *Random Strategy Arnold's Cat Map*

We perform random division on the *N*×*M* image using different squares controlled by a key, and then obtain a series of square blocks. These squares must satisfy two conditions. One is that the union of them covers all pixels. The other is that there is overlapping region between adjacent squares. The first condition ensures that all pixels are scrambled. The second one provides us an opportunity to improve security achieved by using random encryption order. Figure 3, shows an example of random division with six squares.

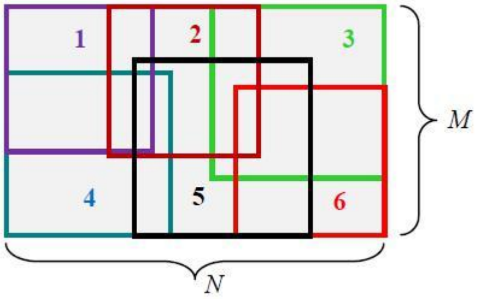


Figure 3. An example of random division

Pixel Muddling: Image scrambling produces an unintelligible or disorder image from the original image. Arnold transform is an efficient technique for position swapping, and widely applied to image encryption. Arnold transform, also called cat map transform, is only suitable for encrypting $M×M$ images. We find that Arnold transform has two weaknesses. One is the periodicity; the other is the requirement that image height must equal image width. The periodicity makes it unsecure, while the requirement limits its applications. To overcome this we use Random Strategy Arnold's Cat Map, which can be used for pixel muddling of $N×M$ images.

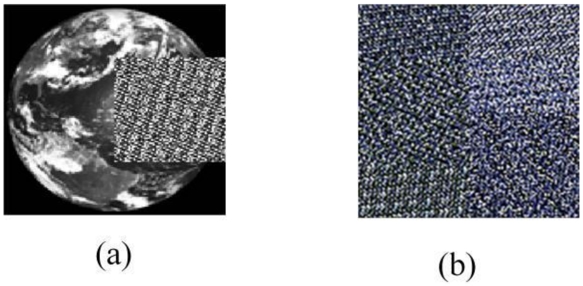


Figure 4. Example of image encryption using Arnold transforms (a) Encryption of a block, (b) Muddled image.

C. Chaos Algorithm

A new kind of color image encryption algorithm based on integrated confusion-diffusion mechanisms and chaos is put forward. Various mathematical operation is conducted between the chosen key feature combinations and the original image with three offset values. Thus, integration confusion with diffusion is achieved. The experimental results demonstrate that this algorithm has advantages of large key space and high security, and moreover, it is sensitive to the secret keys.

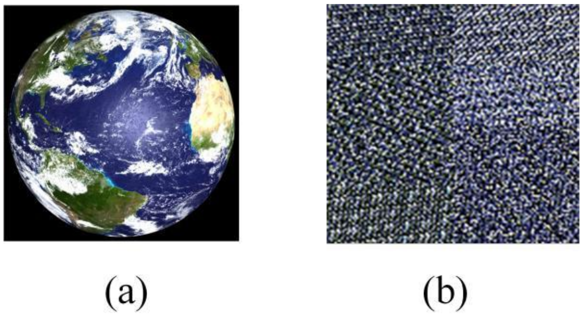


Figure 5. (a) Message Image, (b) Resulting Encrypted Image.

D. Steganography

The existing methods quoted below are done through a survey process. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another". Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements.

1. The cover media that will hold the hidden data.
2. The secret message, may be plain text, cipher text or any type of data.
3. The stego function and its inverse which operates over cover media and the message (to be hidden) to produce a stego media.

During the Steganography process different methodologies for stego formation is tried so that to test which procedure of Steganography formation works good with low level of loss since during Steganography the image will definitely under goes some information loss.

METHODOLOGY 1: Extracting MSB from Message Image which contains 80% of information about the image. Replacing the LSB of the Cover images by means of MSB of message image for each planes independently. Now this image data contains message image's MSB and Cover image's MSB which is known as *Stego Image*. Figure 6, shows an example for this scheme. This category is simulated and found that its visualization is not good, since during extraction of LSB (i.e.MSB of Message image) from stego image results in the loss of 65% of information. This is because the lowest nibble of Message Image is not being saved and hence either 0's or 1's are added in its place.

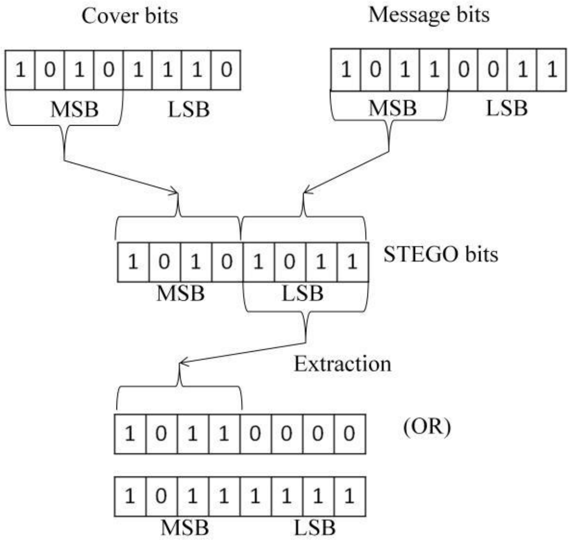
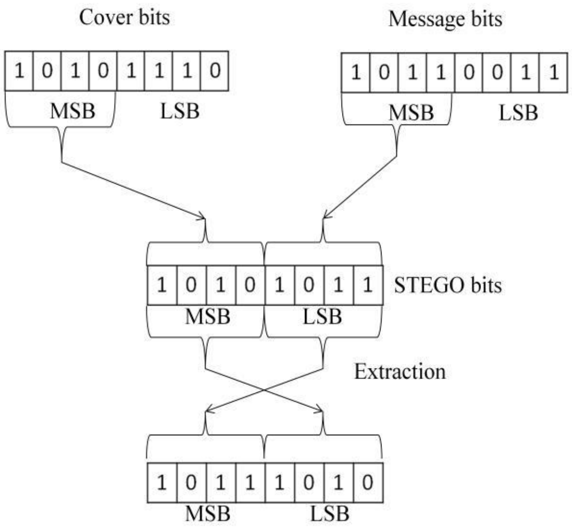


Figure 6. Example for Methodology 1

METHODOLOGY 2: The procedure for this method is same as the Method 1. The only difference is, after extraction the LSB from the Stego image, interchanging of LSB as MSB and MSB as LSB is made, but faced a loss of 45% of information. An example of this scheme is shown in Figure 7.



(b)

Figure 7. Example for Methodology 2.

PROPOSED METHODOLOGY: Resizing the cover image in such a way that number of pixel rows in cover image should be double the size of message image.

1. To preserve the information in message image we have to follow two steps
    a. Extract MSB from Message image and let it be **X**.
    b. Extract LSB from Message image and let it be **Y**.
2. To form a stego image replace X for Cover image first half's LSB and replace Y for Cover image second half's LSB. By doing this we can preserver both MSB and LSB of the message image.

Finally it is found that this Proposed Methodology is much more suitable for chaotic encryption based stego process. A good PSNR after the Extraction and Decryption process is also obtained. From Figure 8, the recovery of both LSB and MSB of Message Image can be analyzed.

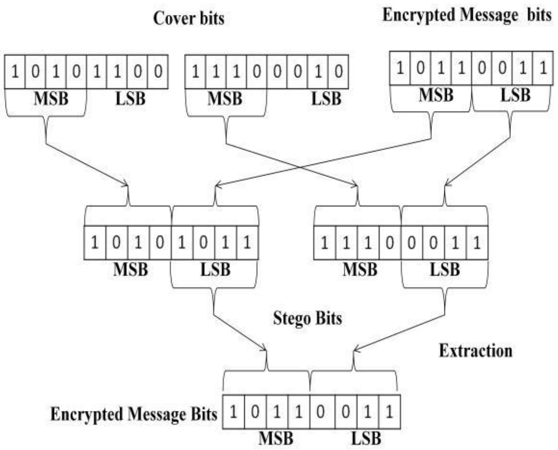


Figure 8. Example for Methodology 3.

Table 1: Comparison of Methodologies

Parameter	Method 1*		Method 2*	Proposed Method*
	0000	1111		
PSNR	28	28	31	∞
TIME (sec)	11	11	12	50
*Values slightly varies for different images				

It is evident from the following Figure 9, that the resulting Stego Image from Proposed Methodology is similar to that of Cover Image. The Stego Image attempts to prevent an unintended recipient from suspecting that the data is there.

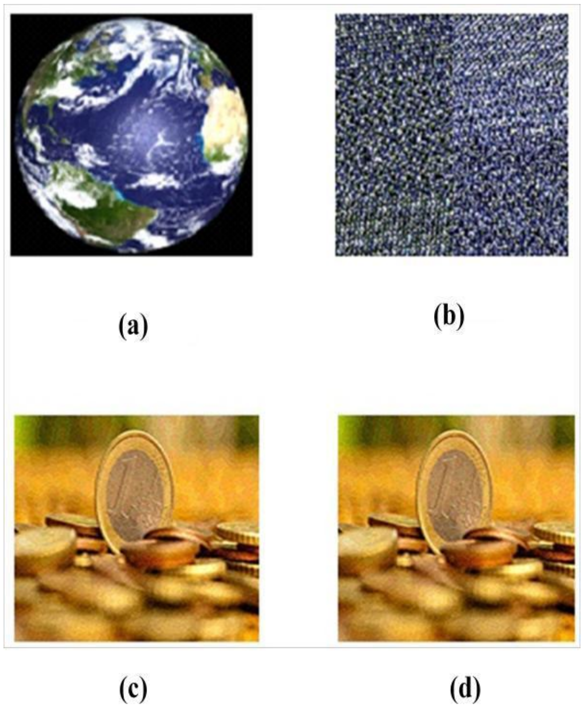


Figure 9. Process of Steganography. (a) Original Image, (b) Encrypted Image, (c) Cover Image, (d) Stego Image.

IV. PRINCIPLES OF DECRYPTION

The principles of decryption algorithm have the following steps:

Step 1: Obtain the Stego Image.
Step 2: Extract the hidden Encrypted Image from the Stego Image using Inverse Stego function by Proposed Methodology.
Step 3: Perform Inverse Chaos Algorithm and Inverse Random Strategy on the Extracted Image using the same key features. Now the original Message Image is obtained.

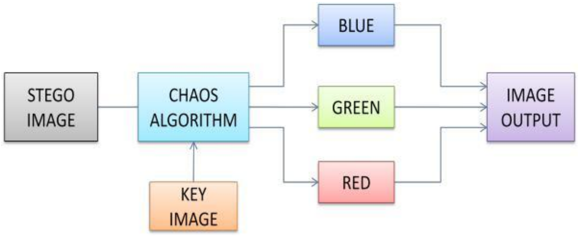


Figure 10. Principle of

Decryption *A. Image Extraction*

The first and foremost step of decryption is image extraction. Bit Plane Separation technique is used to separate the bits which are in combined format. The next step involves the process of bit refinement, that is, MSB bits and LSB bits separately from the Stego Image. This extraction is lossless as mentioned earlier. Figure 11(a), 11(b) shows the Stego Image and the extracted encrypted Message Image respectively.

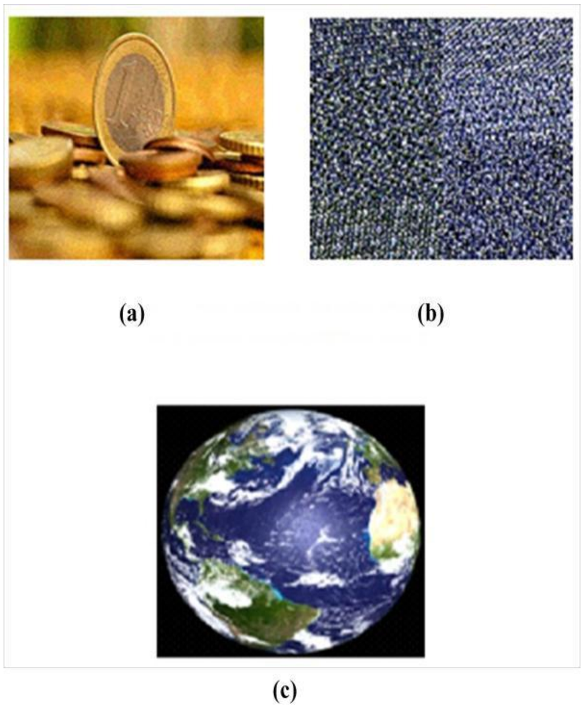


Figure 11. Message Reconstruction. (a) Stego Image, (b) Extracted Image, (c) Reconstructed Original Image.

B. Reconstruction of Message Image

The final stage of decryption includes the use of Inverse Chaos Algorithm and Inverse Random Strategy Arnold's Cat Map. The extracted Image is decrypted by Inverse Chaos Algorithm and then the pixels are re-muddled again by Inverse Random Strategy Arnold's Cat Map to form the original image. This is accomplished by division of decrypted image into six blocks in same order as that of encryption. Figure 11(c) shows the original image after decryption.

V. CONCLUSION

Chaos algorithm and three random strategies of Arnold's transform are combined to design an image encryption scheme. The security of the scheme depends on the random strategies. Since there are many possibilities of random division, iterative numbers, and encryption order, attacker face it difficult to guess all random strategies at the same time. Thus, the security is guaranteed. Although the proposed scheme is based on Arnold transform, it has no size limitation, meaning that it can be applied to encrypt images of any size. This is because the random division can cover all pixels by using a series of squares. Therefore, compared with conventional Arnold transform, the proposed scheme of random strategy is more secure and has more applications. This makes our encryption scheme robust against blocks missing, scratching and Gaussian white noise. In addition, by using Chaos algorithm, more security is ensured because it works only on accurate value and not with approximated value. If there is any change in the value the original image cannot be obtained correctly.

REFERENCES

[1]. Gaurav Prasad and Sujay Narayana, “Two New Approaches For Secured Image Steganography Using Cryptographic Techniques and Type Conversions”,AnInternationalJournal, December 2010.

[2]. Abhijeet A. Ravankar and Stanislav G. Sedukhin, “Image Scrambling Based on a New Linear Transform”, 2011 IEEE.

[3]. Cao Yun and Qiu Run-he, “Integrated Confusion-Diffusion Mechanisms for Chaos BasedImageEncryption”,20114th International Congress on Image and Signal Processing.

[4]. Chen Wei-bin and Zhang Xin, “Image Encryption Algorithm Based on Henon Chaotic System”, 2009 IEEE.

[5]. Fan Jing, Liu Min and Zhu Xian, “Image Scrambling Encryption By Mix Fan Transform Matrixes Technology”, 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012).

[6]. Keun-Moo Rhee, “Image Encryption Using Self Regressive Function”, Fourth International Conference on Networked Computing and Advanced Information Management.

[7]. Liu Wei and Zhang Yun-peng, “Digital Image Encryption Algorithm Based on Chaos and Improved DES”, Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics.

[8]. Qiang Zhang and Shihua Zhou, Xiaopeng Wei, “Image Encryption Algorithm Based on DNA Sequences for the Big Image”, 2010 International Conference on Multimedia Information Networking and Security.

AUTHORS PROFILE

MANI BHARATHI. V is currently pursuing B.E in Electronics and Communication Engineering from P. A. College of Engineering and Technology, Tamilnadu, India. Her area of interests includes Network Security and Cryptography, Image Processing, Digital Signal Processing, Digital Communication.

MANIMEGALAI. M is currently pursuing B.E in Electronics and Communication Engineering from P. A. College of Engineering and Technology, Tamilnadu, India. Her area of interests includes Digital Communication, Network Security and Cryptography, Image Processing, Microprocessors.

SINDUJA. V is currently pursuing B.E in Electronics and Communication Engineering from P. A. College of Engineering and Technology, Tamilnadu, India. Her area of interests includes Network Security and Cryptography, Image Processing, Optical Fiber Communication.