A Novel Image Encryption and Authentication Scheme Using Chaotic Maps

Amitesh Singh Rajput and Mansi Sharma

Abstract. The paper presents an amalgam approach for image encryption and authentication. An ideal image cipher should be such that any adversary cannot modify the image and if any modifications are made, can be detected. The proposed scheme is novel and presents a unique approach to provide two level security to the image. Hashing and two chaotic maps are used in the algorithm where hash of the plain image is computed and the image is encrypted using key dependent masking and diffusion techniques. Initial key length is 132-bits which is extended to 148-bits. Performance and security analysis show that the proposed scheme is secure against different types of attacks and can be adopted for real time applications.

1 Introduction

Storage of data in open networks and information exchange across the internet has created an environment in which illegal users can obtain important information. Images are the most important utility of our life and are used in many applications. In open environments, focusing on processing and transmission of digital images, there are several security problems associated with them. Hence, reliable, fast and robust image security techniques are required to store and transmit digital images. Due to large size of digital images, traditional data encryption algorithms cannot be directly applied to them. An important property of digital images is that they are less sensitive as compared to text data and if some pixels values of the image are modified, the modification cannot be identified by human eye. Therefore, a

Amitesh Singh Rajput
Department of CSE, Sagar Institute of Science & Technology, Bhopal, India
e-mail: amiteshrajput@gmail.com

Mansi Sharma
School of IT, Rajiv Gandhi Proudyogiki Vishwavidalaya, Bhopal, India
e-mail: mansisharma1245@gmail.com

El-Sayed M. El-Alfy et al. (eds.), *Advances in Intelligent Informatics*,
Advances in Intelligent Systems and Computing 320, DOI: 10.1007/978-3-319-11218-3_26

small degradation in the digital image is acceptable which is not possible with text data but this is also an advantage from the attacker's point of view. If an adversary access the image and make some little modifications, the image will be acceptable.

To prevent image from unauthorized access and modifications, strong image encryption and authentication techniques are essential. Image encryption techniques transform the pixel values of the plain image and convert the plain image to another one that is hard to understand. Most applications require confidentiality as well as integrity. Therefore, it is important to develop techniques that are capable of providing both the services simultaneously. To provide authentication, hash functions should be preferred. Using hash functions, integrity of the image is checked and if any modifications have been made, can be determined. Integrity of the received image is checked by comparing the received hash with the one calculated at the receiving end. The general approach to obtain this is to combine encryption and authentication schemes in some way. During the past some years, some image encryption and authentication schemes have been proposed [1, 2, 6].

Another technique for securing digital images is based on the use of chaotic functions. Chaotic techniques provide a good combination of complexity which results into high security, speed and reasonable computational overheads. In order to overcome image encryption problems, a number of different image encryption schemes have been proposed based on chaotic maps [2-5, 7-10, 13-18]. The chaos-based encryption was first proposed in 1989 [9], since then, many researchers have proposed and analyzed a lot of chaos-based encryption algorithms. Two chaotic logistic maps are used in [10]. Initial conditions of both the chaotic maps are calculated using the secret key. Eight different operations are used and at an instance one of them is used to encrypt the pixels of the image. Hyper chaotic functions are used to encrypt the image in [14]. The scheme is divided into two parts. In the first part, total shuffling of the image pixels takes place whereas the shuffled image is then encrypted using hyper chaotic function in the second part. Cryptanalysis of the scheme is presented by [12]. It has been shown that the reuse of the key stream more than once makes the cryptosystem weak against chosen cipher text, chosen plain text attacks. According to [12], three couples of plain text/cipher text were enough to break the cryptosystem in a chosen cipher text and chosen plain text attacks scenario. Two solutions are also projected for changing the key stream. In [15], chaotic image encryption algorithm where key stream is generated by nonlinear Chebyshev function is proposed. The secret keys in encryption process are dependent on each other and provide good correlation results. Diffusion and substitution based gray image encryption scheme is proposed in [11]. The scheme consists of substitution-diffusion techniques. The algorithm is based on the number of iterations (rounds).

To provide more security to the image, authentication and encryption techniques can be pooled. An authenticated image encryption scheme based on memory cellular automata is proposed in [2]. The image is divided into blocks and hash of each block is generated. The encryption is conceded with the linear memory cellular automata (LMCA) to diffuse pixel values of the image. The hash values are used to verify integrity of the image. The scheme proposed in [1] uses digital signature to verify integrity of the received image. The digital signature of the plain image is computed and added to the encoded version of the original image. Image encoding is done by an appropriate error control code, such as Bose Chaudhuri Hochquenghem (BCH) code. A fast image encryption and authentication scheme is proposed in [6]. Message authentication code (MAC) is used to validate integrity of the image. MAC of the plain image is embedded and the entire image is then encrypted using a simple masking function. A novel scheme for image encryption and authentication is proposed in this paper. The rest of the paper is classified as follows: in Section 2, the detailed algorithm of the proposed image cipher is discussed. In Section 3, security and performance analysis of the proposed algorithm is provided. Finally, section 4 concludes the paper.

2 Proposed Approach

The proposed scheme encrypts the plain image and validates integrity of the image at the receiving side. Along with encryption, authentication is also an important aspect for image security and the proposed scheme provides image encryption as well as authentication. The proposed scheme consists of two phases: image encryption phase and, decryption and integrity validation phase.

Chaotic techniques provide a good combination of complexity which results into high security, speed and reasonable computational overheads. Logistic maps have very complicated dynamic behavior. In the proposed scheme, we keep the value of system parameter of both the logistic maps to be constant (3.9999) which corresponds to highly chaotic behavior and we used them to generate initial key stream and provide randomness to the image being encrypted. The two chaotic maps used in the algorithm are –

$$x_{n+1} = 3.9999x_n(1 - x_n) \tag{1}$$

$$y_{n+1} = 3.9999y_n(1 - y_n) \tag{2}$$

A 148-bit key is used in the algorithm. The initial values of both the chaotic maps are computed using the scheme presented by [10] with some modifications. Here, we use 36-bits of the secret key to generate initial values for the first chaotic map. Initial values for the second chaotic map are generated from 24-bits of the secret key. The chaotic maps are executed multiple times, only their initial values are different depending on the key bits selected. The chaotic maps are executed and chaotic values are generated. Initial values of the chaotic maps are different for different phases. Use of diverse values of the chaotic maps in different phases makes the cryptosystem robust such that any adversary cannot obtain meaningful information from the cipher image. The sub-phases of the proposed scheme are explained below.

2.1 Image Encryption Phase

Input: Plain image with initial key
Output: Cipher image with extended key

In the proposed scheme, 512-bit hash of the original image is generated using a standard hash generation technique and generated 512 hash bits are converted into 64 bytes such that each byte represents a decimal number. In this phase, the plain image and initial key are given as input, and encrypted image and extended key are obtained. The initial key length is 132-bits and 16-bits are appended to the key showing the difference value of the hash values and pixels of the plain image. This can be explained as follows.

1. Generate 512-bit hash of the plain image and convert the generated 512-bits into 64 bytes (such that each byte represents a decimal number).
2. Add all the 64 decimal numbers obtained in the last step and store the sum in S_1.
3. Iterate first and second chaotic maps (64 times) and add all the resulting 64 pixel values. Store the sum in $S_{2,}$ and obtain the difference between S_1 and S_2. Convert the difference value into binary form and append the bits at the end of the initial key.

Now, the plain image is encrypted using masking and diffusion techniques. The encryption phase consists of three sub-phases: masking, horizontal diffusion and vertical diffusion. The sub-phases of the scheme are explained below:

2.1.1 Masking Process

In this step, each pixel of the input image is replaced with a new pixel obtained by mixing the properties of the current pixel with the previous pixel and the key stream. The current pixel is added to the previous masked pixel and then the entire sum is XORed with the chaotic key stream generated from the first chaotic map using different set of initial values. Each pixel is masked by the following encryption function –

$$E(i) = M(i) \oplus \{[P(i) + E(i-1)] mod\ L\} \tag{3}$$

Where, P(i) is the plain image pixel value, M(i) is the chaotic key stream generated by executing first chaotic map, E(i) is the encrypted pixel output and L is the gray level. The chaotic key stream is derived from the first chaotic map which is dependent on the key. In this way, all the pixels of the image are masked resulting a masked image.

2.1.2 Horizontal Diffusion

Diffusion refers to the process of rearranging or spreading out the pixels in the image so that redundancy in the image is spread out over the complete cipher image. The masked image obtained in the previous phase is given as input in this segment. In horizontal diffusion, we mix the properties of horizontally adjacent pixels of the plain image and XOR them concurrently with the resulting values of the first chaotic map. In an image cryptographic system, the process of diffusion removes the possibility of differential attacks which is done by comparing the pair of plain and cipher images.

2.1.3 Vertical Diffusion

Here, the image obtained in last step is given as input. Like horizontal diffusion, here we mix the properties of vertically adjacent pixels of the input image and XOR them concurrently with the same resulting values of the first chaotic map as of horizontal diffusion respectively. Complete cipher image is obtained as output of this phase.

2.2 Image Decryption and Integrity Validation Phase

Input: Cipher image
Output: Detecting whether the received image is tampered or not.

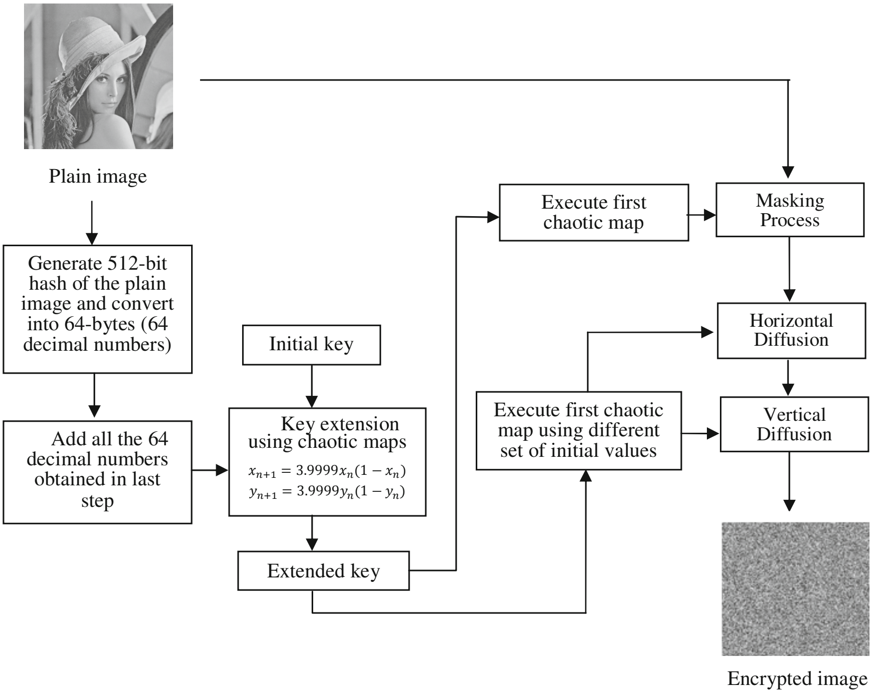

Plain image
Generate 512-bit hash of the plain image and convert into 64-bytes (64 decimal numbers)
Add all the 64 decimal numbers obtained in last step
Initial key
Key extension using chaotic maps
$x_{n+1} = 3.9999x_n(1 - x_n)$
$y_{n+1} = 3.9999y_n(1 - y_n)$
Extended key
Execute first chaotic map
Execute first chaotic map using different set of initial values
Masking Process
Horizontal Diffusion
Vertical Diffusion
Encrypted image

Fig. 1 Block diagram of the proposed scheme

The reverse process of encryption is applied to the cipher image to get the recovered plain image. Integrity of the received image is tested out here. The steps of this phase are explained below.

1. Extract the decimal value from the last 16 bits of the key (say D_1).
2. Generate 512-bit hash of the recovered plain image and convert these 512-bits into 64 bytes such that each byte represents a decimal number and add all the 64 decimal numbers obtained. Store the sum in S_3.

3. Execute first and second chaotic maps (64 times), and add all the resulting pixel values and store the sum in S_4 and obtain the difference value (D_2) between S_3 and S_4.

Compare D_1 and D_2 for integrity. Use the same hash generation algorithm as used at the sender side. If D_1 and D_2 are equal, then integrity of the recovered image is validated.

3 Performance and Security Analysis

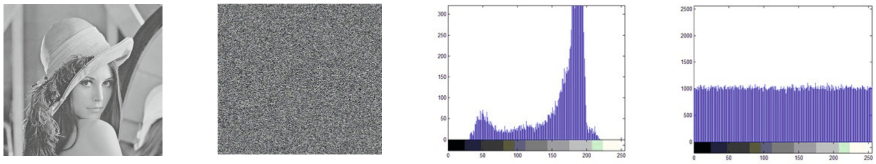
An ideal image cryptographic scheme should resist all kinds of attacks. In this section, security and performance of the proposed image cryptographic scheme are discussed.

3.1 Key Space Analysis

Key space of a cryptosystem should be fairly large such that it can resist brute-force attacks. The total number of keys that can be used in the scheme defines the key space. The key used in image cipher should be neither too long nor too short. In the proposed scheme, key length is 148-bits. The initial key length is 132-bits which is then further extended to 148-bits. The last 16 bits of the secret key represents difference value of the generated hash values and image pixel values. The 148-bit key length causes 2^148 different combinations (3.5×10^44) which is sufficient to resist various brute-force attacks.

3.2 Statistical Analysis

The encrypted image should possess certain random properties such that it can resist statistical attacks which are quite common now days. To evaluate robustness of the proposed scheme, some tests have been performed and results are shown in the next sub sections.



(a) (b) (c) (d)

Fig 2. Histogram analysis: Frames (a) and (b) show the plain image ‘Lena’ and its corresponding cipher image respectively. Frames (c) and (d) show histogram of images shown in (a) and (b).

3.2.1 Histogram

Histogram of the encrypted image should be distributed uniformly showing that the pixels of the encrypted image are fairly distributed. We performed this test on the plain image ‘Lena’. The histogram of the plain image and its corresponding encrypted image are shown in figure 2. The histogram of the encrypted image shows fair distribution of pixels which does not reveal any information to the adversary.

3.2.2 Correlation of Adjacent Pixels

Neighboring pixels are highly correlated in images. Correlated pixels can be horizontally, vertically or diagonally adjacent. For an ideal image cipher, the less correlation of two adjacent pixels is the stronger ability of resisting statistical attacks. The proposed scheme exhibits this property well. In this section, the correlations between horizontally, vertically and diagonally adjacent pixels of the plain and encrypted image are discussed. The correlation between adjacent pixels is calculated by the following equations:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{4}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{5}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{6}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}} \tag{7}$$

Where x and y are gray-scale values of two adjacent pixels of the image, cov(x, y) is the covariance, D(x) is the variance and E(x) is the mean. In order to test correlation between two adjacent pixels, we selected 3600 random pairs of adjacent pixels (horizontal, vertical and diagonal) of the original and encrypted image. Table 1 illustrates the comparison between the proposed scheme and scheme presented by [15] and shows that the proposed scheme exhibits good correlation results than [15].

Table 1 Correlation coefficients of two adjacent pixels of the plain image ‘Lena’ and corresponding encrypted image

	Plain image (Lena)	Encrypted image by the proposed scheme	Encrypted image by [15]
Horizontal	0.9189	0.0006	-0.09736
Vertical	0.9028	-0.0057	0.04844
Diagonal	0.9266	-0.0077	-0.07068

3.3 Differential Analysis

The changes in cipher image should be significant such that known-plaintext attack and chosen-plaintext attack can be avoided. Two common measures: number of pixels change rate (NPCR) and unified average changing intensity (UACI) are calculated to test how one pixel change in the plain image affects the corresponding cipher image. The percentage of different pixels in two encrypted images is calculated by NPCR. On the other hand, the average of intensity – difference between the pixels of two cipher images is measured by UACI. The NPCR and UACI are calculated by the following equations:

$$NPCR = \frac{\sum_{ij} D(i,j)}{W \times H} \times 100 \tag{8}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{ij} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100 \tag{9}$$

Where C_1 and C_2 are two encrypted images, whose corresponding original images have only one-pixel value difference. D (i, j) is a two dimensional array of the same size as of C_1 or C_2. D (i, j) is derived from C_1 and C_2. If C_1 and C_2 are equal, D (i, j) =0, otherwise D (i, j) =1. W and H are width and height of the image. We applied the proposed scheme over a number of images of the USC-SIPI image database and find that the proposed scheme exhibits NPCR ≥ 99%. Hence, the scheme exhibits good properties to resist differential attacks. The NPCR and UACI test results are shown in table 2 and 3 respectively.

Table 2 NPCR

Image name	NPCR (%)
Boat	99.0435
Lake	99.4996
Lena	99.5011
Pepper	99.5941

Table 3 UACI

Image name	UACI (%)
Boat	33.2626
Lake	33.0106
Lena	33.0998
Pepper	33.1628

3.4 Performance Analysis

For an ideal image cipher, encryption/decryption time and computational complexity of the algorithm is an important aspect. Images are of large size as compared to the text, hence chaotic techniques are used. Due to large size of the images, time is an important aspect to be considered when developing an image cipher. In the previous sections, we have already shown that the proposed scheme is good for resisting different kind of attacks. The proposed scheme consists of iterating chaotic maps and the operations involved in the scheme consists of simple addition/subtraction and XORing, yet the scheme is robust against different types of attacks. Hence, the proposed scheme is efficient in terms of computational complexity. Time analysis has been done on 2.30 GHz i3-2350M CPU, with 2 GB RAM computer. The operating system is Windows 7 and programming environment is MATLAB 7.7. The size of the image is 124×124. The average encryption speed of the proposed scheme is 90 ms which shows that the proposed scheme is good in terms of execution time as well.

4 Conclusion

Images are the most important utility of our life. They are used in many applications. Ideal image security techniques should be such that any adversary cannot modify the image and if any modifications are made can be detected. In the paper, we proposed a novel approach to provide confidentiality and integrity to the image. Hash of the plain image is generated and then the entire image is encrypted using masking and diffusion techniques which are key dependent. Initially 132-bit key is used in the algorithm which is further extended to 148-bits. A significant feature of the proposed scheme is that integrity of the image is checked which is not achieved with most image encryption schemes. Experimental, security and performance analysis shows that the scheme is secure against different types of attacks and can be adopted for real time applications. In future, the proposed scheme can be extended to provide more security to the image using some mathematical models and more arbitrary chaotic functions.

References

1. Sinha, A., Singh, K.: A technique for image encryption using digital signature. Optics Communications 1, 229–234 (2003)
2. Bakhshandeh, A., Eslami, Z.: An authenticated image encryption scheme based on chaotic maps and memory cellular automata. Optics and Lasers in Engineering 51(6), 665–673 (2013)
3. Chen, G., Mao, Y., Chui, C.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals 21, 749–761 (2004)
4. Kwok, H.S., Tang, W.K.S.: A fast image encryption system based on chaotic maps with finite precision representation. Chaos, Solitons and Fractals 32, 1518–1529 (2007)
5. Shateesh Sam, I., Devraj, P., Bhuvaneshwaran, R.S.: A novel image cipher based on transformed logostic maps. Springer Science + Business Media, LLC (2010)
6. Qiu, J., Wang, P.: An image encryption and authentication scheme. In: 2011 Seventh International Conference on Computational Intelligence and Security (CIS), December 3-4, pp. 784–787. IEEE (2011)
7. Sabery, M., Yaghoobi, M.: A New Approach for Image encryption using Chaotic logistic map. 978-0-7695-3489-3/08 ©. IEEE (2008)
8. Mao, Y., Chen, G., Lian, S.: A novel fast image encryption scheme based on 3D chaotic baker maps. Int. J. Bifurcat. Chaos. 14, 3613–3624 (2004)
9. Matthew, R.: On the derivation of a chaotic encryption algorithm. Cryptologia 8(1), 29–42 (1989)

10. Pareek, N.K., Patidar, V., Sud, K.K.: Image encryption using chaotic logistic map. Image Vis. Comput. 24, 926–934 (2006)
11. Pareek, N.K., Patidar, V., Sud, K.K.: Diffusion-Substitution bsed gray image encryption scheme. Digital Signal Processing 23(3), 894–901 (2013)
12. Rhouma, R., Belghith, S.: Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Physics Letters A 372, 5973–5978 (2008)
13. Sun, F., Liu, S., Li, Z., Lu, Z.: A novel image encryption scheme based on spatial chaos map. Chaos Solitons Fractals 38, 631–640 (2008)
14. Gao, T., Chen, Z.: A new image encryption algorithm based on hyper-chaos. Physics Letters A 372, 394–400 (2008)
15. Huang, X.: Image encryption algorithm using chaotic Chebyshev generator. Nonlinear Dyn. 67, 2411–2417 (2012)
16. Wei, X., Guo, L., Zhanga, Q., Zhang, J., Lian, S.: A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. The Journal of Systems and Software 85, 290–299 (2011)
17. Zhang, Q., Guo, L., Wei, X.: Image encryption using DNA addition combining with chaotic maps. Math. Comput. Model. 52, 2028–2035 (2010)
18. Shatheesh Sam, I., Devaraj, P., Bhuvaneswaran, R.S.: An intertwining chaotic maps based image encryption scheme. Nonlinear Dyn. 69, 1995–2007 (2012)