Image Encryption and Authentication Scheme using 3D Chaotic Map

Pragati Thapliyal
Mtech student
DIT University
India

Madhu Sharma
Assistant Professor
DIT University
India

ABSTRACT
Cryptographic techniques are in demand due to vast development in application of information transmission and communication. Image encryption and authentication schemes have been continuously studied to meet the demand of secure image transmission through networks. A number of effective chaos-based image encryption and authentication schemes have been proposed. The intent of this paper is to propose an image encryption and authentication scheme using chaotic map. Arnold cat map is used for diffusion as well as for substitution. This paper applies an alternate structure of the classic block cipher applied with Arnold Cat map is used for encryption and hash function is used for Authentication purpose. The paper that is being followed uses a keyed hash function is introduced to generate hash values from both the plain-image and the secret hash keys[1], which leads to large computational time, whereas our schemes computational time is less as compared to the previous. The experimental results show that the proposed encryption technique is efficient and has high security features.

Keywords
Arnold Cat map, Authentication, Chaotic Maps, Image Encryption.

1. INTRODUCTION
In today's IT age, communication has an important role and impact on the growth of technology. The computer security has continuously involved in making communication more rife and robust. The very basic task of cryptography is to provide confidentiality by different encryption methods. Security mainly consists of three parts namely data confidentiality, data integrity and data authenticity. The data confidentiality is the protection of data from unauthorized disclosure. The data integrity is defined as the assurance that the data received are exactly as sent by an authorized entity. The authentication is the assurance that the communication entity is the one that it claims to be [7]. A mechanism is a need for security and privacy of data that is transferred over the electronic media. Either the communication media is wired or wireless, protection is needed from the unauthorized access of information. The method of transforming the original information into an unreadable format is called Encryption and the reverse process is called Decryption of information. The study of encryption and decryption is known as Cryptography.

Cryptography is the method of protection of privacy of data during communication, under threatening conditions. A process in which data is protected from destroying or from unauthorized access is called data protection. Data protection could be provided on different ways. One of them is cryptology, it consists of both cryptography and cryptanalysis. Cryptography involves the study and the applications of the principles and techniques by which the information is rendered unintelligible to all but the intend to receive. It is an effective way for protecting sensitive information as it is stored on the media and transmitted through non trusted network communication paths. Cryptography is used to create and use methods for transformation of data, information or messages in order to make that transformed message visible only for precise, desired person. Breaking and exploiting the characteristics of cryptographic method in order to get information is known as cryptanalysis.

Chaotic maps are simple, unstable, dynamical systems with high sensitivity to initial conditions. Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks [16]. Traditional image encryption [2] algorithm such as data encryption standard (DES), has the weakness of low-level efficiency when the image is large. The chaos-based encryption [4] has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. Images are used in distinct areas such as medical, military, science, engineering, art, entertainment, advertising, education as well as training.

In classical encryption schemes, encryption and decryption algorithms depend on the same secret key. These encryption methods are called symmetric-key encryption schemes. DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm, AES (Advanced Encryption Standard) etc. are some of the symmetric encryption schemes. But they has the weakness of low-level efficiency when the image is large [5]-[6]. The chaos-based encryption [2]-[3] has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. The chaotic system is rich in significance and in implication because of sensitivity to change initial conditions, control parameters, ergodicity, random-like behavior, repeated processing and very high diffusion and confusion properties that are desirable for cryptography.

The chaotic system is rich in significance and in implication because of sensitivity to change initial conditions, control parameters, ergodicity, random-like behavior, repeated processing and very high diffusion and confusion properties that are desirable for cryptography [14]. With the fast evolution of digital data exchange, security of information becomes much important in data storage and transmission. Due to the increasing use of images in industrial processes, it is essential to protect confidential images from unauthorized access.

Chaos based cryptosystem plays a crucial role research of information security and number of chaos based image encryption and authentication algorithms has been proposed. In general, many digital image services require reliable security in storage and transmission, due to which the individual appreciation and privacy differ from a person to

person. The reason for the image encryption and encryption is to transmit the image securely over the network so as to protect it from unauthorized user.

1.2 Encryption

There are two types of cryptographic schemes in use today: private key or secret key (also known as symmetric) cryptography and public key (also known as asymmetric) cryptography. Symmetric key cryptography uses the same key for encryption and decryption. Another type of encryption method, asymmetric or public key cryptography uses different keys to encrypt and decrypt. On one hand, asymmetric key cryptography requires more computation resources than symmetric key cryptography does, on the other hand, symmetric key cryptography is difficult for key deployment and management. Though most framework use one type of cryptography, there still exist some schemes that use both asymmetric-key and symmetric-key cryptography.

1.3 Authentication

Authentication is a service related to identification of entity and information itself. In entity auth the claimant must identify itself to the verifier. The fundamental task of cry is to provide confidentiality by encryption methods. The messages to be transmitted can be any kind of data. In many environments, it is more important that communications be authenticated rather than encrypted. That is, both parties should be convinced of each other's identity. It is needed to establish identity and verify identity before allowing access to resources.

The authentication parameters comprises of hash functions, message authentication code and digital signature [8]. Cryptographic hash function is a one way compression function that maps an arbitrary length message to a fixed length value. Any change in the input data will result in the hash value to change. Message authentication code uses a cryptographic hash in conjunction with a shared secret to check integrity. Only one holding the shared key can modify the data [9]. Digital signature is based on public-key ciphers and provides non-repudiation. A digital signature is usually signed by a private key and can be verified by its public key. With the sender's signature, the receiver can believe the message was sent by the claimed sender and the sender cannot claim he did not sign a message when he also claims that his private key remains secret [10].

1.4 Hash Function

In cryptography hash functions are basic building block for many security applications like integrity protection, message authentication, digital signature schemes, password storage and protection, confirmation of commitment, pseudo-random string generation and key derivation. A hash function which can be categorized as a well-defined procedure or mathematical function patterns which convert a variable-sized large amount of data into a small datum which might be a single integer that acts as an index to perform an array related function. The output of a hash function is called hash value, message digest, or fingerprint [16].

MD5 was proposed by R.Rivest in 1992 as a strengthen version of MD4. Both MD4 and MD5 produce 128-bit message digest. SHA has the design principle of MD4. SHA-0 was developed in 1993 by National Security Agency as the Secure Hash Standard and SHA-1 was introduced in 1995 as a revision of SHA-0. SHA-1 was issued by NIST as FIPS PUB 180-1. Both SHA-0 and SHA-1 produce a message digest of 160-bit. NIST introduced new hash function standard FIPS PUB 180-2 in 2002. Three new hash functions, SHA-256, SHA-384 and SHA-512, collectively known as SHA-2, have been specified in this standard. Later on another hash function SHA-224 was added to this standard [11].

1.5 Arnold Cat Map

Arnold's Cat Map is named after the Russian mathematician Vladimir Arnold, who discovered it in 1960s using an image of a cat. Arnold's Cat Map is a transformation that can be applied to an image. The pixels of the image appear to be randomly rearranged, but when the transformation is repeated enough times, the original image will reappear. Equivalently, in matrix notation, this is

Equivalently, in matrix notation, this is

$$\Gamma\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod 1$$

The original image of the cat is sheared and then wrapped around in the first iteration of the transformation. After some iterations, the resulting image appears rather random or disordered, Arnold's cat map is a simple discrete system that stretches and folds the trajectories in phase space, which is another typical feature of chaotic processes. The phase space for this simple system can be represented by a square, and the stretching and folding process scrambling effect is relatively best in Arnold's Cat Map. The Arnold Cat Map takes concepts from linear algebra and uses them to change the positions of the pixel values of the original image. The result after applying the Arnold Cat Map will be a shuffled image that contains all of the same pixel values of the original image [15].

2. THE PROPOSED SCHEME

The proposed scheme is an alteration of the one suggested by Zhang Yi, WANG and Huaqian Yang, Kwok-Wo at al. In their system, two a general cat-map is used for permutation and diffusion, as well as the OCML (one-way coupled map lattice), which is applied for substitution. These two methods are operated alternately in every round of encryption process [1]. In our altered method the original images should be partitioned or merged into N× 2N pixel blocks at first. In doing so, the proposed algorithm encrypts an N × 2N plaintext block into an N × 2N ciphertext block. Image is divided into four parts and hash is calculated on each part using different techniques i.e. MD5 and SHA for authentication purpose.

The details are:

1. Image is divided into four parts each part is used to calculate the hash values.
2. Hash is calculated using MD5, SHA 12, SHA 32 and SHA 128 on the four parts.
3. Now for encrypting the image take the image pixels as an input.
4. Partition the N× 2N plaintext block into two N × N left and right parts.
5. Shuffle the pixels of image using cat map.

6. Now the output generated from step 2 is xored with the remaining pixels from the image.

7. The output from step 4 will serve as an input for the next round.

8. Reiterate steps 2−5 to execute n rounds of encryption.

9. After retaining original image it is further divided into four parts and hash is calculated in the same manner as step 2.

10. Compare the hash values from step 2 and 9.

3. ALGORITHM

The image encryption and authentication algorithm is based on the Arnold cat map and Hash function.

Step1. I read an image
Step2. I reads img1, img2, img3 & img4 image partitions
Step3. h reads hashmap of img1 (MD-5)
Step4. h1 reads hashmap of img2 (SHA-1)
Step5. h2 reads hashmap of img3 (SHA-256)
Step6. h3 reads hashmap of img4 (SHA-512)
Step7. Ii convert I into gray scale
Step8. ccfo stores correlation coefficient of Ii
Step9. imgX create zero matrix of the size of original matrix
Step10. imgX2 create another zero matrix of the size of original matrix
Step11. [NoPixelnY, c] stores row, column and dimension of image
Step12. for l 1← to 4
Step13. for i ← 1 to NoPixel loop through all the pixels to generate cat map
Step14. for j ← 1 to nY
Step15. Imgi get new row coordinate [(m+n) mod NoPixel]
Step16. Imgj get new column coordinate [(m+2n) mod NoPixel]
Step17. imgX(Imgi,Imgj,:) store image pixel value in new Coordinates from original coordinate
Step18. endfor
Step19. endfor
Step20. for i ← 1 to NoPixel
Step21. for j ← 1 tonY
Step22. imgXx(i,j,:) add 245 to pixel value;
Step23. endfor
Step24. endfor
Step25. newXx reads bit xor image
Step26. I reads newXx replace original image with generated image
Step27. endfor
Step28. Reverse steps 12 through 27 to get decrypted image
Step29. ccfEimage reads calculate correlation coefficient of encrypted image
Step30. Iccf reads calculate correlation coefficient of decrypted image
Step31. ccfdenc reads correlation coefficient of decrypted and original image
Step32. Dimage reads Dimg1, Dimg2, Dimg3 &Dimg4 image partitions
Step33. Dh reads hashmapof img1 (MD-5)
Step34. Dh1 reads hashmapof img2 (SHA-1)
Step35. Dh2 reads hashmapof img3 (SHA-256)
Step36. Dh3 reads hashmapof img4 (SHA-512)
Step37. if h is equal to Dh then display Hash matches
Step38. results reads calculate NPCR and UACI on Original and Decrypted image

4. RESULTS

The proposed encryption algorithm is implemented in MATLAB for computer simulations. The algorithm will accept and image as input data.

The below figures (1), (2), (3) and (4) represents the original image, its histogram and the encrypted image and its histogram respectively.

Figure 1 Original Image

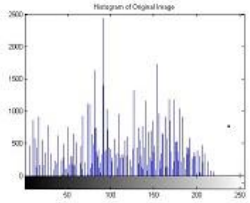

Figure 2 Histogram of Original

Figure 3 Encrypted Image

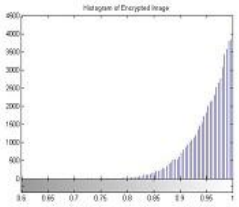

Figure 4 Histogram of Encrypted

4.1. Correlation Coefficient

Correlation coefficient 'r' is the measure of extent and direction of linear combination of two random variables. If two variables are closely related, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related. The coefficient r can be calculated by the following formula:

$$r = cov(x, y)/(\,D(x)\,D(\,y))$$

The Table 1 below shows the results of correlation coefficient between two adjacent pixels.

Table 1. Correlation Coefficient

Direction	Plain Image	Encrypted Image
Horizontal	0.982113	0.027823
Vertical	0.987628	0.016238
Diagonal	0.973402	-0.01189

4.2 Differential Attacks:

Differential attack would become ineffective if a tiny change in the plain-image causes a significant difference in the cipher- image. To measure this capability quantitatively, the following measures are usually used: number of pixels change rate (NPCR) and unified average changing intensity (UACI). They are defined as follows [12]:

$$\mathrm{D(i,j)} = \begin{cases} 0, c^1(i,j) = c^2(i,j) \\ 1, c^1(i,j) \neq c^2(i,j) \end{cases} \quad (1)$$

$$\mathrm{NPCR} = N(c^1, c^2) = \frac{\Sigma i,jD\,(i,j)}{T} \times 100\% \quad (2)$$

$$\text{UACI} = U(c^1, c^2) = \frac{\sum i,j \left| c^1(i,j) = c^2(i,j) \right|}{F \times T} \times 100\% \quad (3)$$

Table 2: NPCR and UACI

Images	NPCR	UACI
Lena	98.6013	33.453
Baboon	98.5921	33.463
Peppers	99.5059	33.421

5. CONCLUSION

An Image encryption and authentication algorithm using chaotic map and hash values is discussed in this paper. The proposed system will work efficiently for image encryption and authentication. The algorithm is based on the concept of shuffling the pixels positions and diffusion through Arnold Cat map and hash functions are used for the purpose of enshrining authenticity. The scheme is more time efficient and hence effective in current scenario as compared to the previously proposed schemes. Use of multiple diffusions in the encryption scheme and multiple hash functions make the cryptosystem more secure, rife and robust. Its cryptographic qualities have been evaluated through different statistical analyses. The chaos-based image encryption and authentication scheme can be applied to video data as well.

6. ACKNOWLEDGMENTS

I am thankful to my supervisor Mrs. Madhu Sharma Assistant Professor of the Department of Computer Science and Engineering for her proper guidance and valuable suggestions throughout the course of this paper. If not for the above mentioned people, my paper would never have been completed in such a successfully manner. I once again extend my sincere thanks to all of them.

7. REFERENCES

[1] Huaqian Yang, Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang, Pengcheng Wei, 2010, A fast image encryption and authentication scheme based on chaotic maps, Elsevier,.

[2] Zhang YiWei, WANG YuMin2 & SHEN XuBang. June 2007, A Chaos-Based Image Encryption Algorithm Using Alternate Structure, Sci China Ser F-Inf Sci, vol 50(3), pp 34-341, ,

[3] Huang Yuanshi, Xu Rongcong, Lin Weiqiang. 2006, An Algorithm for JPEG Compressing with Chaotic Encrypting, in Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation ,CGIV'06,

[4] Changjiang Zhang. 2008, Digital Image watermarking with Double Encryption by Arnold Transform and Logistic, Fourth International conference on Networked Computing & advanced information Management, pp. 329-334,

[5] Nikhil Debbarma, Lalita Kumari, and Jagdish Lal Raheja. August 2013, 2D Chaos Based Color Image Encryption Using Pseudorandom Key Generation, IJETTCS volume 2, Issue 4.

[6] Chen GR, Mao YB**.** 2004, A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps. Chaos, Solitons & Fractals 2004, vol 21, pp 749–61.

[7] Chiaraluce F, Ciccarelli L. 2007, A New Chaotic Algorithm for Video Encryption. IEEE Trans Consum Electron 2002, vol 48, pp 838–43,.

[8] William Stallings, 2006, Cryptography and Network Security**,** 4th ed. Pearson, , ch. 1, pp. 18-19.

[9] Menezes A., van Oorschot P., Vanstone S., 1997 ,Handbook of Applied Cryptography, CRC Press,.

[10] Bakhtiari S., Safavi-Naini R., Pieprzyk J., 1995, "Cryptographic Hash Functions: A Survey", Technical Report 95-09, Department of Computer Science, University of Wollongong,.

[11] Diffie W., Hellman M. 1976, "New Directions in Cryptography", IEEE Transaction on Information Theory, vol. 22, no. 5, pp. 644-654.

[12] NIST, Secure Hash Standard (SHS), 2002, Federal Information Processing Standards 180-2.

[13] Chen Guanrong, Mao Yaobin, Chui Charles K.. 2004, A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Soliton Fract.

[14] Pragati Thapliyal, Madhu Sharma, 2015, A image encryption scheme using chaotic maps.

[15] H Tiwari, 2014, Design of Cryptographic Hash Functions based on MD and MD Variant.