4th International Conference on Latest Trends in Engineering, Science, Humanities and Management
Indian Federation of United Nations Associations, Qutab Institutional Area, New Delhi (ICLTESHM-17)
07 May 2017, www.conferenceworld.in ISBN : 978-93-86171-37-5

IMAGE ENCRYPTION AND AUTHENTICATION USING REPETITIVE APPLICATION OF LINEAR TRANSFORMATIONS& MD5

Ajay Raj Parashar[1], Surbhi Lakhani[2], Mansi Gautam[3]

[1,2,3] *Information Technology Department, Hindustan College Of Science & Technology (India)*

ABSTRACT

Security and confidentiality of data or information at the present time has become an important concern. Advanced methods for secure transmission, storage, and retrieval of digital images are increasingly needed for a number of military, medical, homeland security, and other applications. Various kinds of techniques for increase security data or information already is developed, one common way is by cryptographic techniques. Cryptographic algorithm often used today and the proven strength specially the digital image is Algorithm with Chaos system. To provide authentication then at the receiver side we use Additional algorithm namely Message Digest 5 (MD5).

This research aims to optimize security bitmap image format by combining the two algorithms namely Chaos-based algorithms and MD5 algorithm into one application. Experiments conducted show that the proposed algorithm possesses robust security features such as fairly uniform distribution, and plain images, almost ideal entropy, and the ability to highly de-correlate adjacent pixels in the cipher images. Furthermore, it has a large key space, and transform image to pure text file which greatly increases its security for image encryption applications.

I. INTRODUCTION

Information that can be read and implicit without any special procedures or method is termed as plaintext or clear text. The technique of concealing plaintext in order to hide its particular material is called encryption. The impression of encryption is to make a message incomprehensible, except to the receiver.

Data encryption technology is used to benefit protection against loss, exploitation or alteration of private information. Encrypting plaintext results in indecipherable rubbish called cipher text. Encryption is used to guarantee the hidden information from anyone of concern not intended to, even those who can comprehend the encrypted data. The procedure of backsliding cipher text to its original plaintext is considered as decryption. Popular encryption algorithm used in image is the Chaos -based encryption. Chaos System used varies, like Logistic Map, Baker Map, Arnold Cat Map, and others. Logistic Map is one of Chaos is an encryption system that is simple but produce complex calculations, requiring short processing time, do not have a period and has sensitivity to initial input value. Because some excess algorithm Chaos in image encryption, the authors tried to apply the algorithm Chaos Logistic system uses to perform encryption Map the RGB pixel image, and added to

ISBN : 978-93-86171-37-5

the algorithm Arnold Cat Map that is used to perform randomization the pixel position of the image, which is expected to be obtained cipher image which has scrambled pixel perfect and not can be recognized.

Cipher image generated from a single cryptographic algorithm is not strong enough to withstand the attack cryptanalyst; this is due to an increase in computation speed more quickly. To be able to increase the strength of the cipher image, we needs to be encrypting image using a combination of encryption algorithm and authentication algorithm that produced the cipher strength of the encryption process can be guaranteed, and can hold the attack from cryptanalyst.

In 1992 professor Ronald Rivest of MIT designed a message digest algorithm known as MD5.This algorithm is used to verify data integrity through the creation of a 128 bit message digest from data input of any length.These algorithms do factoring very large numbers which make it safe. Today, MD5 is used in cryptographic applications from banking, and e-mail security to e-commerce on the Internet.

II. SCOPE OF THE PROJECT

Analysis indicates that the scheme is secure and authenticate as well. To get the original image is to solve the encryption algorithms which are Chaos-based algorithm.

This will make the strength of the cipher can be assured and the simplicity of the proposed scheme makes it easy to implement in software.

Encryption is the most reliable way to secure data. National security agencies and major financial institutions have long protected their sensitive data using cryptography and encryption. Today the use of encryption is growing rapidly, being deployed in a much wider set of industry sectors and across an increasing range of applications and platforms. Put simply, cryptography and encryption have become one of the hottest technologies in the IT security industry – the challenge now is to ensure that IT organizations are equipped to handle this shift and are laying the groundwork today to satisfy their future needs

It is clear that the protection of personal or private data is critical to the wellbeing of any company that stores or processes this information. Encryption has become a last line of defence for data protection because, once data is encrypted, if stolen or even simply misplaced, it is rendered unreadable without the keys to decrypt that data.

The future of encryption is brighter than ever before. The demand for more control and protection of corporation information assets and third-party information is increasing dramatically. The amount of information being communicated and stored electronically is vastly greater than even five years ago. As a result, the need for more effective information security products is growing at a higher rate than any other aspect of IT technology within the enterprise today. The Internet and the mobility of its users have removed the perimeters of communication. Encryption is the last line of defence for the modern day enterprise. But the underlying growth isn't necessarily in basic encryption technologies. Although there have been recent new encryption algorithms released (Advanced Encryption Standard in the U.S., for example), the mathematics of cryptography—along with the key exchange technologies that have been deployed—are quite satisfactory for most of today's applications. In fact, many products from PGP Corporation and others utilize a number of encryption and key exchange algorithms that best suit particular customer needs.

ISBN : 978-93-86171-37-5

II. PROPOSED MODEL

The proposed model is based on the combination of two algorithms, i.e.

1. Arnold Cat Map
2. MD5

This model provides a securely encrypted image along with the authenticity to the receiver. Image can be encrypted by using the algorithm named Arnold Cat Map and for the authenticity, MD5 algorithm is being used here. Sender will send the encrypted image with the hash of that image to the receiver. At the receiver end, receiver will generate the hash of the received image and verify with the hash sent by the sender. If the hash generated by receiver matches with the received hash, then image will be accepted, otherwise image will be rejected.

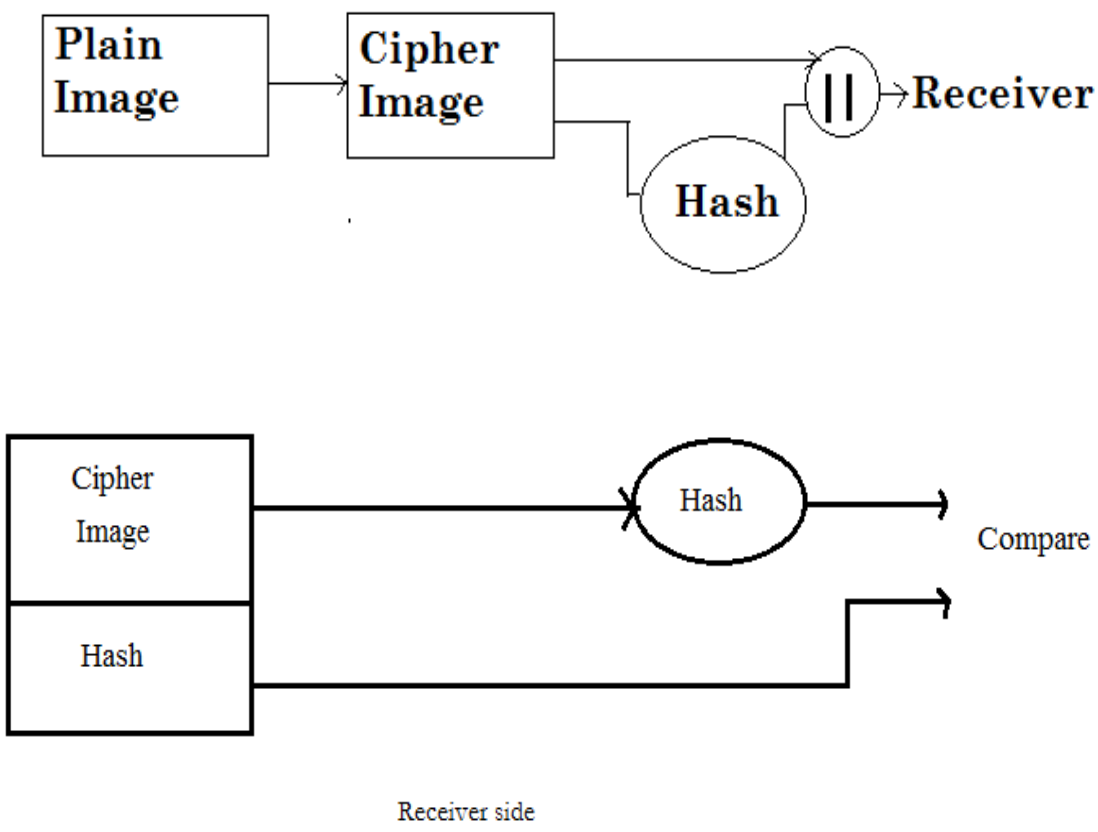
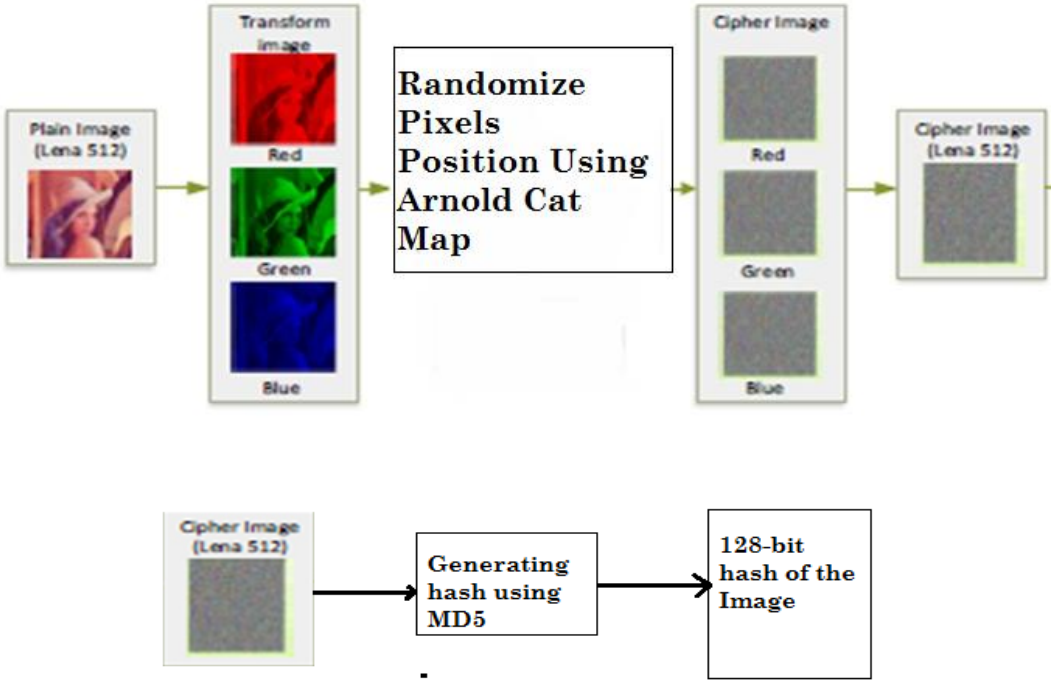


Fig.1 General diagram of the proposed system

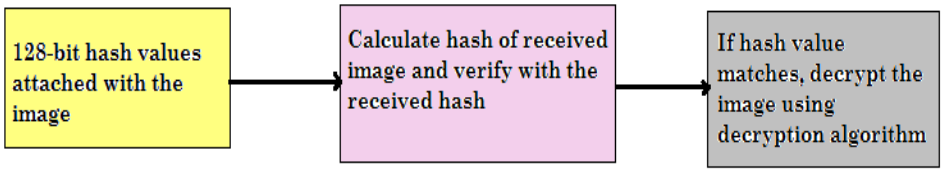
ISBN : 978-93-86171-37-5

III. ENCRYPTION



IV. DECRYPTION

At receiver end, receiver will get the hash attached with the encrypted image.



V. ALGORITHMS

5.1 ARNOLD CAT MAP

Arnold Cat Map (ACM) is a two-dimensional chaotic map after discovered by Vladimir Arnold in 1960 .ACM transform the coordinates (x, y) in the image of size N × N to the new coordinates (x ', y'). The equation of ACM is :

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(N)$$

ISBN : 978-93-86171-37-5

The inverse equation of ACM is :

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} mod(N)$$

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 is more apparent if we placed a picture of a cat in the square. One can then see the time evolution of the system by observing how the cat gets stretched, cut up, and then placed back into the square. From the figure below, we observe that typically, any two points that are initially very close together quickly become separated fromeach other after repeated applications of the map. Image data have strong correlation among adjacent pixels. Statistics analysis on large amounts of images shows that averagely adjacent 8-16 pixels are correlative in horizontal, vertical, and also diagonal directions for both natural and computer graphical images. In order to disturb the high correlation among pixels, we adopt Arnold cat map to shuffle the pixel positions of the plain image.

Let’s understand the algorithm using an example,

Suppose N=100 & a=1, b=1

And Position of pixels be x=2, y=3

DestinationMatrix[(2+3)%100][(2+2*3)%100]= SourceMatrix[2][3]

- ⇨ [5%100][8%100]
- ⇨ [5][8]

In the proposed system, we have used 15 transformations of the image to get the encrypted image that means the numerical process will be repeated 15 times. It can be changed according to the user’s requirements.

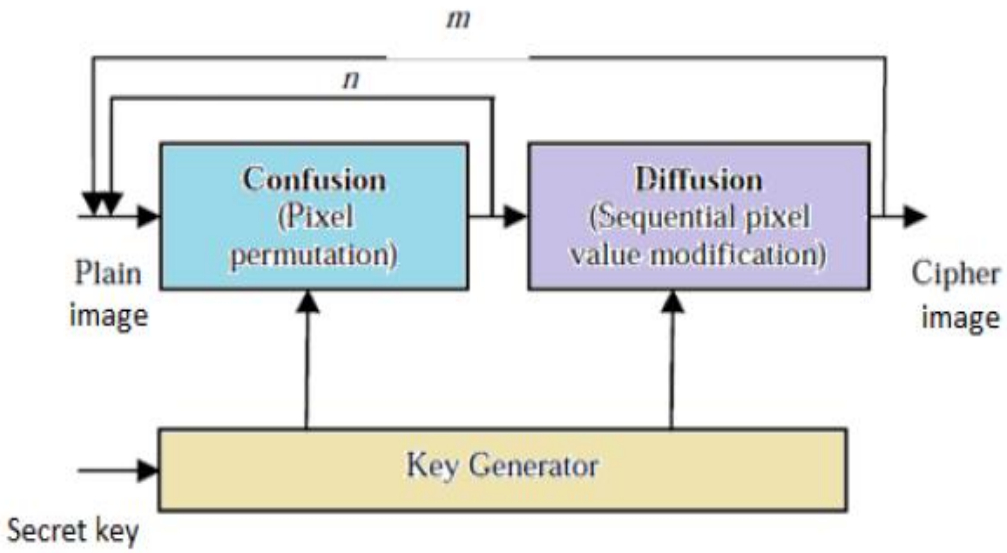


Fig.2 Typical Architecture of Chaos Based Cryptosystem

ISBN : 978-93-86171-37-5

Fig.3 Original Image

Fig.4 Encrypted Image

Fig.5 Decrypted Image

1.1.1 ENCRYPTED IMAGE AT SLIGHTLY DIFFERENT RATE OF TRANSFORMATIONS

Fig.6 : 0 Transformations

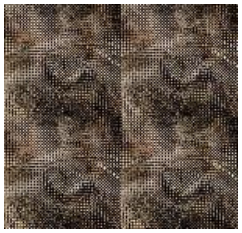


Fig.7 : 100 Transformations

ISBN : 978-93-86171-37-5

Fig.8 Original Image

Fig.9 Encrypted Image

Fig.10 : 20 Transformations

Fig.11 : 256 Transformations

ISBN : 978-93-86171-37-5

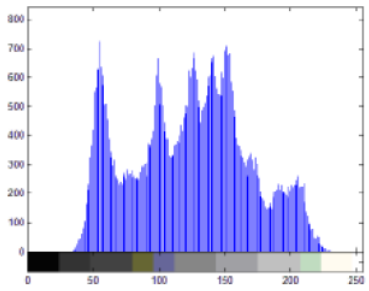


Fig.12 Histogram of Original Image

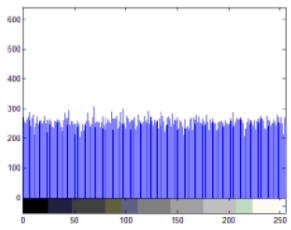


Fig.13 Histogram of Encrypted Image

5.2 MD5

- In 1992 professor Ronald Rivest of MIT designed a message digest algorithm known as MD5.
- This algorithm is used to verify data integrity through the creation of a 128 bit message digest from data input of any length.
- These algorithms do factoring very large numbers which make it safe.
- Today, MD5 is used in cryptographic applications from banking, and e-mail security to e-commerce on the Internet .

5.2.1 WORKING OF MD5 :

1. Appending Padding Bits. The original message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512.
2. Appending Length. 64 bits are appended to the end of the padded message to indicate the length of the original message in bytes.
3. Initializing MD Buffer. MD5 algorithm requires a 128-bit buffer with a specific initial value..
4. Processing Message in 512-bit Blocks. This is the main step of MD 5 algorithm, which loops through the padded and appended message in blocks of 512 bits each. For each input block, 4 rounds of operations are performed with 16 operations in each round.

5.2.2 AUTHENTICATION USING MD5

We will comparethehash value of sent image with received image.

Hash value of the image to be sent:

ISBN : 978-93-86171-37-5

98896e62aadd3fd65dcd52129596130b

Hash value of received image:

98896e62aadd3fd65dcd52129596130b

VI. PERFORMANCE ANALYSIS

S. No.	Features	Proposed System
1.	Security	Uses Independently developed algorithm.
2.	Confidentiality	Algorithm for implementing secrecy is used.
3.	Key Concept	No key used.
4.	Attack Prevention	Prevents attacks and tapping
5.	Authenticity	Uses message digest 5 to provide authenticity

VII. INTERFACE

➢ Browse the image from the system.

ISBN : 978-93-86171-37-5

- By pressing the encrypt button, we will get a frame, by pressing confirm button, an encrypted image will be generated.

- Image will be displayed in the image box.

ISBN : 978-93-86171-37-5

- Now by pressing MD5 button, we will generate the hash of the encrypted image and send it to the user along with the image.
- Image can be decrypted by pressing decrypt button.
- Receiver will verify the hash value, if matched, image will be accepted, else rejected.

VII. FUTURE DEVELOPMENT

We can improve the Graphical User Interface (GUI) of the application. It can be further implemented on PDF files, Word documents, etc.

VIII. CONCLUSION

As confidential data like banking information, military information, some transaction details etc. hence security of data is of great concern. In this system, the combination of algorithms is proposed to secure as well as authenticate the data that is being received.

REFERENCES

[1] International Journal of Computer Applications (0975 – 8887) Volume 123 – No.6, August 2015

[2] El- Fishawy, N., & Abu Zaid, O. M. (2007). Quality of encryption measurement of bitmap images with RC6, MRC6, and rijndael block cipher algorithms. International Journal of Network Security.

[3] Faragallah, O. S. (2011). An efficient block encryption cipher based on chaotic maps for secure multimedia applications. Information Security Journal: A Global Perspective.

[4] El- latif, A. A. A., Li, L., Zhang, T., Wang, N., Song, X., &Niu, X. (2012). Digital Image Encryption Scheme Based on Multiple, 67–88. doi:10.1007/s11220-012-0071-z

[5] Gaur, E. A., & Gupta, E. M. (2014). Review : Image Encryption Using Chaos Based algorithms