Image Encryption Using Meitei Lock Sequence Generated from Hash Functions

Yumnam Kirani Singh

C-DAC Silchar,
Ground Floor, IIPC Building NIT Silchar Campus,
yumnam.singh@cdac.in

Abstract*: *Proposed here is a secure image encryption scheme based on generalized Vigenere cipher and Meitei Lock Sequence (MLS) generated from standard hash functions. MLS is a unique random sequence of any length greater than 2 generated from a non-negative array having two or more elements. It is unique in the sense that no two arrays can generate the same sequence however close or similar the two arrays are. In other words, when there is any slight change in any of the input array, the generated MLS's are drastically different. Also, the length of the sequence can be as infinitely long. These properties make MLS a good key string for a secure encryption scheme. SHA(Secure Hashing Algorithm) or any hash code generator has desirable feature which can be used for generation of MLS. In a hash code generator, it produces unique fixed length sequence from any input string, if there is any slight change in the input, the generated output will be totally different. This feature is made used of in generating an MLS of any desired length for use in the proposed image encryption scheme. Experimental results show that the proposed encryption scheme is a secure encryption scheme. The correlation coefficient between the original image and encrypted images are negligibly small indicating that there is no trace of original image information in the encrypted image. Also, the correlation coefficients between the original image and decrypted images with wrong passwords which are close to the encryption password are also negligibly small. These show the tightness of the key system in the encryption scheme.

***Keywords*: Meitei Lock Sequence, Hash Functions, SHA-1, SHA256, SHA512, Image Encryption, Symmetric Cryptography, Generalized Vigenere Cipher, Correlation Coefficients.**

(Article history: Received: 14th December 2019 and accepted 16th June 2020)

I. INTRODUCTION

Encryption is the process of encoding information in unintelligible form so that only authorized people can render it intelligible through a process called decryption. Encryption and decryption is performed with the help of a key or keys. Security of an encryption system also dependent on the difficulty of guessing or derivability of the key. The more the search space of the key, the more secure is the encryption system. For example, 128 bit key encryption system is considered less secure as compared to 512 bit or 1024 bit key encryption system. There are numerous standard encryption schemes such as DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), AES (Advanced Encryption Standard) for encrypting textual information. But the development of internet technology, we have to deal with other forms of information such as image, video and audio. Of these, image is the most frequently used information type in the internet world through social media such as Facebook and WhatsApp. So, there is a requirement of developing strong encryption scheme to prevent the misuse of images posted on the internet.

Image is highly correlated data, unlike text data. Encryption schemes used for encrypting text data such as DES, AES, etc. are not suitable for suitable for encrypting images [4]. Also, the public encryption scheme such as RSA or ECC are not suitable for encryption of image because they are too slow to be used in encryption of large volumes of data in an image. In order to encrypt an image, the correlation of the pixels in the original image need to be reduced significantly before applying any encryption method. That is, image encryption requires an effective distorter function or scrambler [4, 5, 6] to de-correlate pixels in an image. Several reversible transforms such as Fourier Transform (FT), Discrete Cosine Transform (DCT), etc. as a distorter function for image encryption [8]. But the problem of using FT and DCT as distorter functions is that trace of image appears even when password are quite different during decryption. Many people use chaotic mapping as distorter function for image encryption [5, 7, 10]. But the security of these chaotic mapping based encryption schemes are yet be widely accepted. Some other uses DNA sequence operation [2,3] or Cellular automata as distorter functions [7, 9].

In this paper, an encryption scheme is proposed which is simple, fast and secure. The encryption scheme does not require any distorter function or chaotic mapping. It is based on generalized Vigenere cipher which uses random look-up tables for encryption and decryption. This makes the decryption and encryption process very fast. Moreover, it uses MLS (Meitei Lock Sequence) [12, 13, 14] which can be considered as one-time pad lock to secure the encryption scheme. The MLS's can be generated from the recursive call of SHA functions [11] from any randomly chosen password. As SHA function can take any size input, the search space for

password is infinitely large. This will make the brute force search for password impossible because the password length is not fixed. The encryption scheme has been tested for traceability of the image inform from the decrypted image by using decryption passwords which are slightly different from the encryption password. It is found that there is no trace of original image in the decrypted image when there is any difference in the password. The correlation coefficients of the original image and decrypted images of wrong passwords have been computed and they are found to be negligibly small. This indicates that the proposed encryption scheme is secure from which getting the recognizable information of the original image from the encrypted image is only possible when the decryption password is exactly same as the encryption password.

II. GENERATION OF MLS FROM HASH FUNCTIONS

Security of an encryption scheme lies in the key or the password. If the password can be guessed or traced through mathematical or statistical analysis, it cannot be used for a secure encryption scheme. Hash functions such as MD5, SHA1, SHA256, SHA512 etc. which generate hash code of particular length from a given input can be used to generate a secure password string like MLS from which tracing of input is impossible. In this paper we are using the SHA algorithms SHA1, SHA256 and SHA512 by recursively calling them to generate an MLS of desired length. The steps for generating an MLS sequence from a hash function is given below.

1. Compute M, the number of pixels in the image
2. Find L, the length of the hash code generated by the hash function
3. Find K =Ceiling(2M/L), the number of times a hash function is to be repeated to generate at least M random values.
4. Read an input password string
5. Assign KeySequence to an empty array
6. Generate the hash code from a particular hash function
7. Convert the hash code to integer sequence by taking two successive characters
8. Concatenate the integer sequence to KeySequence
9. Use Hash code as next input string
10. Continue 6 to 8 K times

The MLS generated from hash functions are quite random in nature and there is no trace of periodicity in the generated MLS. The waveforms generated from the same password 11111 from the three different hash functions SHA1, SHA256 and SHA512 are shown in Fig. 1, Fig.2 and Fig.3 respectively.

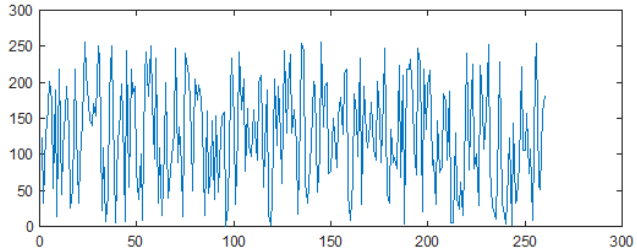

Fig.1: MLS generated from SHA1 using password 11111

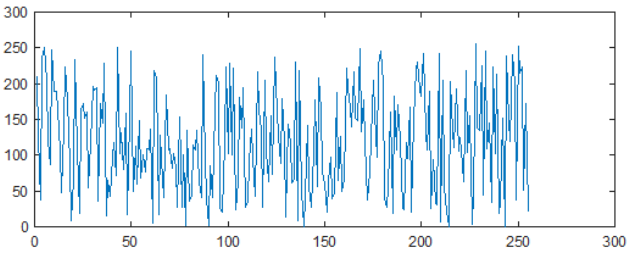

Fig.2: MLS generated from SHA256 using password 11111

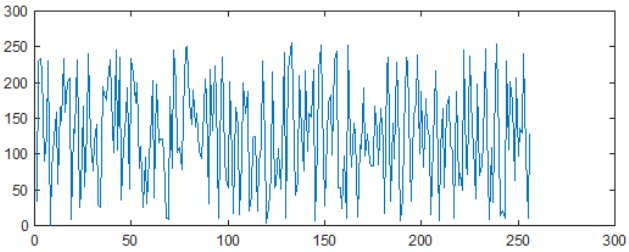

Fig. 3: MLS generated from SHA512 using password

From the figures, it is clearly seen that the generated sequences from are random in nature and there is no trace of periodic repetition in any part of the generated sequence. Such feature is desirable for generating a key sequence for use in a secure encryption scheme.

III. IMAGE ENCRYPTION USING MLS

Here, we will be using generalized Vigenere cipher [14] for encrypting and decrypting image. As images are highly correlated data, we need to use a highly randomized encryption and decryption table along with the MLS sequence generated from the hash functions. In generalized Vigenere cipher, any random table whose rows or columns are unique can be used as encryption table. We can generate infinitely many such random tables which once generated cannot be generated again. The encryption is performed based on this random table but not in the input image. In other words, the encrypted image is formed by the values of the random encryption table not the pixel values of the image. So, there is hardly any correlation between original image and encrypted image, i.e., there is no visible or distinguishable trace of the original image in the encrypted image. This avoids the necessity of using any distorter function or chaotic map in the image encryption using generalized Vigenere Cipher. The process of encryption using Vigenere cipher is very simple, just like using a look-up table. This makes the encryption scheme very fast.

Let E be the encryption table, I is the image, K is the key matrix generated from a password. Then, the encrypted image C, is obtained as

C=E(I,K)

The process of decryption is also very simple and fast. It uses a decryption table D derived from the encryption table E. The process how the decryption table is derived from encryption table is described in [4]. These two tables (E and D) are inverse to each other. That is, any one of them can be used for encryption or decryption. When one is used for encryption, the other must be used for decryption.

So, if D is the decryption table corresponding to the encryption table E, then the original image I can be obtained from encrypted image C using the following relation.

I=D(C, K)

The random encryption and decryption tables of size 256x256 are shown in Fig. 4 and Fig. 5. Since, the image range is 0 to 255, the encryption table is sufficient to encrypt gray and color images whose pixels are in the range 0 to 255. For color image encryption, each color plane is encrypted with the same encryption table and the same MLS. Similarly, for decryption each color plane of the encrypted image is decrypted with the same decryption table and same MLS.

Another important feature that makes the proposed encryption scheme highly secure is the use of MLS K as the key for encryption. The MLS K is generated from a password of any desired length greater than 1.i.e., there is no upper bound of the length of the key. This makes the key search space is infinitely large and extremely difficult for to apply brute force to search the password.

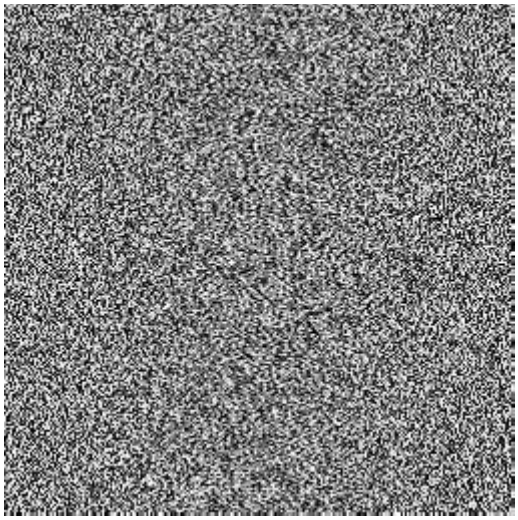

Fig. 4: Image of Encryption Table E of size 256x256

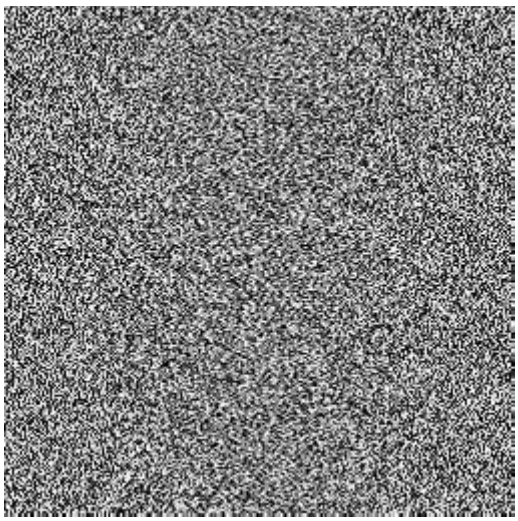

Fig.5: Image of Decryption Table D of size 256x256

IV. Experimental Results

For experimentation, we consider the image_0204 from the Frontal face dataset Collected by Markus Weber at California Institute of Technology, which can be downloaded from the internet. The reason for choosing the image is that most regions in the image have uniform pixel distribution. Such an image is difficult to encrypt to hide the visible trace of highly correlated regions. For experimentation, the original image size is reduced to 0.25 percent so that it can be placed properly in the paper without adjusting its size and at the same image does not occupy large space. The reduced image is then converted to gray scale image as shown in Fig.6. Three different MLS's are generated from password 11111 using hash functions SHA1, SHA256 and SHA512 to encrypt the image. The encrypted images using these three MLS's are shown in Fig.7, Fig.8 and Fig.9 respectively. From these figures, it is seen that there is no trace of intelligible information present in the encrypted images. Also, we compute the correlation between the original image and the encrypted images. The correlation coefficients are negligibly small as shown in second column of Table-1.

Fig. 6: Original Image

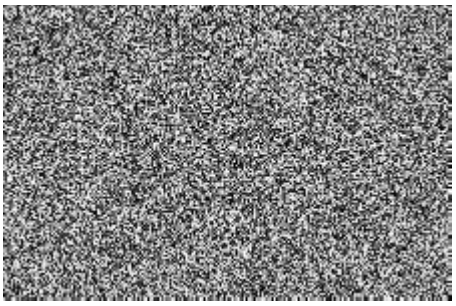

Fig. 7: Encrypted image with MLS (11111) from SHA1

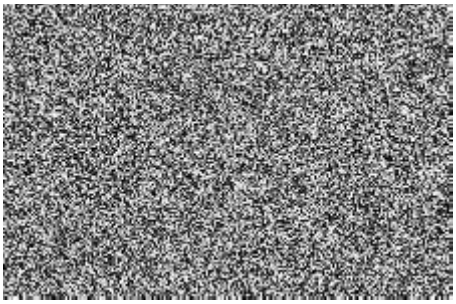

Fig.8: Encrypted Image with MLS(11111) from SHA256

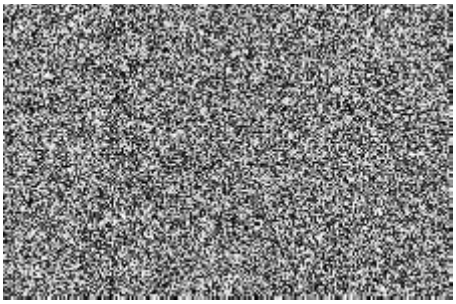

Fig. 9: Encrypted Image with MLS(11111) from SHA512

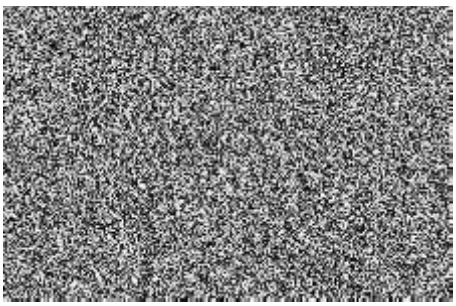

Fig.10: Decrypted Image with MLS(111) from SHA1

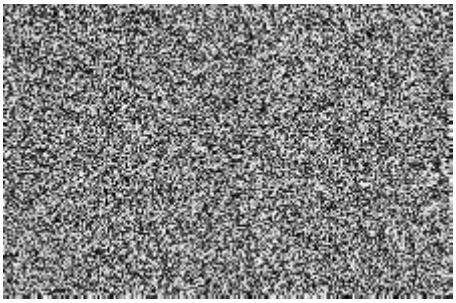

Fig. 11: Decrypted Image with MLS(11110) from SHA256

The encrypted images are then decrypted with passwords which are close to the encryption password (11111) to test whether any trace of information of the original image appear in the decrypted image when use with wrong passwords however close they are to encryption key. It is found that the decryption images are totally random and unintelligible as long as there is any slight difference in the decryption password. Correlation coefficients are computed between the original images and the decrypted images with MLS's generated from SHA1, SHA256, and SHA512 using passwords 11, 111, 1111, 11101, 111011 and 10111 as shown in 3rd to 9th columns of Table-1. It is seen that the correlation coefficients are negligibly small which indicate that there is no trace of information between the original and the decrypted image where there is any difference in the decryption password from the encryption password. The decrypted image corresponding to MLS (111) generated from SHA1 which gives the largest negative correlation value is shown in Fig.10. Also, the decrypted image corresponding to the least negative correlation value when decrypted with the MLS (11110) generated using SHA256 is shown in Fig. 10. From these two figures, we see that the decrypted images having negative correlation values are all random and unrecognizable.

Fig. 12: Original Color Image

Fig. 13: Encrypted image with MLS(11111) from SHA1

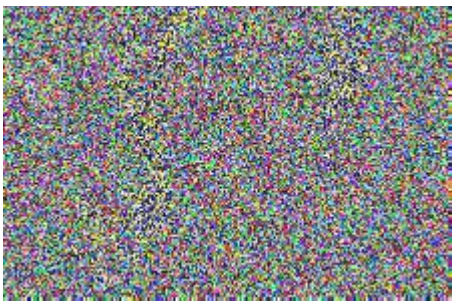

Fig.14: Encrypted image with MLS(11111) from SHA256

.Table-1: Correlation coefficients of encrypted images and decrypted images with original gray image

MLS from Hash function	Correlation Coefficients between original Image and							
	Encrypted Image with password	Decrypted images with passwords						
	11111	11	111	1111	11110	11101	11011	10111

SHA1	-0.0043	-0.0020	-0.0066	-0.0029	0.0025	0.0018	-0.0065	0.0103
SHA256	0.0100	-0.0043	0.0116	0.0023	-9.3051e-04	0.0044	0.0036	0.0146
SHA512	0.0070	0.0030	0.0037	0.0018	0.0031	-0.0036	-0.0057	-0.0038

Fig. 15: Encrypted image with MLS(11111) from SHA512 correlation

We also test the encryption scheme for color image. The color image used in the experimentation is shown in Fig. 12. Since a color image has three color planes - Red, Green and Blue planes, each color plane is separately encrypted using the MLS's generated from SHA1, SHA256, SHA512 from the same password 1111. The encrypted color images are respectively shown in Fig. 13, Fig. 14 and Fig. 15. It can be seen that the encrypted color images are totally random and there is no trace of intelligible information of the original image in these encrypted images. To measure the similarity between the original color image and the encrypted color images, the correlation coefficients between the color planes of the original image and the color planes of the encrypted image are computed and are given in the second column of Table-2.

Also, the encrypted images are then decrypted with MLS's generated from SHA1, SHA256 and SHA512 with slightly different passwords to test whether any trace of intelligible information appears in any of decrypted images with wrong passwords. The decrypted images with wrong passwords are totally random and unintelligible. The correlation between the color planes of the original image and the color planes of the decrypted images using wrong passwords are computed and are provided in 3rd to 9th columns of Table-2. It can be observed that the correlation coefficients are negligibly small. In other words, the decrypted color planes are unintelligibly random and hence the decrypted color images.

Table-2: *Correlation coefficients of color planes of encrypted images and decrypted images with original color image*

MLS from Hash function	Correlation Coefficients between original Image and							
	Encrypted Image with password	Decrypted images with passwords						
	11111	11	111	1111	11110	11101	11011	10111
SHA1	0.0003 -0.0015 0.0025	0.0005 0.0018 -0.0026	0.0018 0.0062 -0.0015	0.0010 -0.0023 0.0051	-0.0070 0.0081 - 0.0048	0.0175 -0.0101 0.0040	0.0040 0.0098 0.0067	0.0055 -0.0090 -0.0063
SHA256	0.0079 0.0034 0.0013	-0.0032 0.0060 0.0012	-0.0033 0.0095 0.0022	0.0041 0.0078 -0.0033	0.0001 0.0026 0.0068	-0.0052 0.0064 0.0020	0.0060 0.0036 0.0001	-0.0049 0.0032 -0.0010
SHA512	-0.0052 0.0048 0.0118	-0.0088 0.0086 -0.0007	-0.0081 -0.0076 0.00004	-0.0082 -0.0060 -0.0005	-0.0022 0.0025 0.0067	0.0069 0.0103 0.0021	0.0011 0.0021 0.0061	0.0018 0.0006 0.0079

V. CONCLUSIONS

A secure image encryption scheme based on generalized Vigenere Cipher and Meitei Lock sequences generated from standard hash functions has been described. The proposed scheme does not require any distorter or chaoticmap as a preprocessing step to de-correlate image pixels before applying encryption. The security of the encryption scheme depends on the use generalized Vigenere cipher and MLS generated from SHA functions. The generalized Vigenere use random encryption and decryption tables which is more powerful than confusion and diffusion technique used in a secure encryption scheme. As a result the encrypted images are random images with no trace of distinguishable information of the original image. Similarly, the decrypted images become random images when there is slight change in the password. This makes the known plain text attack impossible. Moreover, the search space for password is infinitely large which makes the brute force attack next to impossible. In short, the proposed image encryption scheme is a simple, fast and secure encryption scheme.

REFERENCES

[1] Souyah A, Faraoun KM (2016) An image encryption scheme combining chaos-memory cellular automata and weighted histogram. Nonlinear Dyn 86(1):639–653

[2] Norouzi B, Mirzakuchaki S (2017) An image encryption algorithm based on DNA sequence operations and cellular neural network. Multimed Tools Appl 76(11):13681–13701

[3] Xiuli Chai , Yiran Chen, Lucie Broyde (2017) A novel chaos-based image encryption algorithm using DNA sequence operations. Opt Lasers Eng Volume 88, pp. 197–213

[4] Hua Z, Yi S, Zhou Y (2018) Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process 144:134–144

[5] Li S, Zhao Y, Qu B et al (2013) Image scrambling based on chaotic sequences and veginère cipher. Multimed Tools Appl 66(3):573–588

[6] Zeng L, Liu R, Zhang LY, Liu Y, Wong K-W (2016) Cryptanalyzing an image encryption algorithm based on scrambling and veginere cipher. Multimed Tools Appl 75(10):5439–5453

[7] Niyat AY, Moattar MH, Torshiz MN (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt Lasers Eng 90:225–237

[8] Lala Kirkor, Sami Baba, Thawar Arif, Zayad Shaban, "Image Encryption using DCT and Stream Cipher", European Journal of Scientific Research, Volume 32.,No. 1, pp. 48-58, 2009.

[9] Wang Y, Zhao Y, Zhou Q, Lin Z (2018) Image encryption using partitioned cellular automata. Neurocomputing 275:1318–1332

[10] Zhang Y (2018) The image encryption algorithm based on chaos and DNA computing. Multimed Tools Appl 77:1–27

[11] Avinsh Kak, "Lecture Note: Hashing for Message Authentication" https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture15.pdf

[12] Y. K. Singh, S.K. Parui, "Simplet and Its application in Signal Encryption", Multidimensional Systems and Signal Processing, Volume 15, Issue 4, October 2004, pp. 375-394

[13] Y. K. Singh, A Simple, fast and secure Cipher, ARPN Journal of Engineering and Applied Sciences, Volume 6, No. 10, pp. 61-69.

[14] Y. K. Singh, "Generalization of Vigenere Cipher", ARPN Journal of Engineering and Applied Sciences, Volume 7, no. 1, 2012, pp. 39-44.

AUTHOR PROFILE

YumnamKirani Singh completed Master's Degree in Electronics Science from Guwahati University in 1997 and got Ph. D. degree from Indian Statistical Institute, Kolkata in 2006. Served as a lecturer in Electronics in Shri Shankaracharaya College of Engineering & Technology from Jan 2005 to May 2006. Joined CDAC Kolkata in May 2006 and worked there before coming to CDAC Silchar, in March 2014. Developed Bino's Model of Multiplication, ISITRA, YKSK Transforms and several other image binarization and edge detection techniques. Interested in working in the application and research areas of Signal Processing, Image Processing, Pattern Recognition and Information Security. Also published several papers in national and international journals and conferences