DESIGN OF HIGHLY AVALANCHE CHAOTIC IMAGE ENCRYPTION SCHEME BASED ON MODIFIED SHA-1

[1]Subham Jain, [2]Prof. Nitin Saxena

[1]M. tech. Scholar, [2]Professor
[1,2]JEC, Jabalpur

***Abstract*: The paper work is a new approach in the hashing area, which use a modified SHA-1 image Encryption/ hashing with modifier round proposed design has come up with idea of using 40 rounds instead of 80 round of SHA-1, that will increase the speed of hash generation for achieving that proposed work simply modified the single compression/iteration operation. The results of security analysis such as statistical tests, differential attacks, key space, key sensitivity, entropy information and the running time are illustrated and compared to recent encryption schemes where the highest security level and speed are improved.**

***Keywords:* AES-Advance encryption System, SHA-Secure Hash Algorithm, NPCR-Number of Pixels Change Rate, UACI-unified averaged changed intensity**

I-INTRODUCTION

Protection of multimedia data from unauthorized access became a serious and important issue in various aspects of daily life . The data of image could also be used and explored by hackers that it may cause uncountable losses for the owner of images. To avoid these problems, it has become necessary and imperative to encrypt digital image using techniques and algorithm of encryption before send them. We found various schemes and algorithms of encryption such as the traditional encryption methods like RSA (Rivest, Adi Shamir and Leonard Adleman), DES (Data Encryption Standard, AES (advanced encryption standard), etc demonstrate low levels of security and also very weak anti attack ability due to some intrinsic features images such as the strong correlation between adjacent pixels, size and high redundancy. Moreover, these algorithms based on discrete mathematics which are very complex to use and require more resource of time computation and power to implement them in embedded dispositive. To provide a better solution to image security problems, many encryption schemes and algorithms have been proposed such as which use the chaotic systems that provide a good combination of speed and security level.

Our approach is to propose a fast and secure scheme for digital image encryption using only two-diffusion process based on nested chaotic attractor and the Secure Hash Algorithm SHA-1 to generate a secret key. The main advantages of our chaotic sequence used are the efficiency, simplicity and rapidity, all these features are very important it can be implemented on embedded systems.

II-METHODOLOGY

Figure 1shown below is the flow of proposed image Encryption with hashing here modified SHA-1 and a new proposed method is used. The steps of proposed design are as below:-
Step1: Input a image of any format and covert image into pixels using MATLAB
Step 2: Convert 2D or 3D image into 1D discrete format using resize function
Step 3: Apply Proposed Encryption with a 64 bit key on the image segment the sub-image is of 8 pixels or 64 bit
Step 4: Apply modified SHA-1 on the encrypted sub-image and develop Hash of sub-image
Step 5: Do the same process for all sub-images of main image and construct final Hash.
Step 6: Concatenate the Hash and original image.
Step 7: At the receiver end again develop the Hash function of the image as the same process as was discussed in the step1 to step 5.
Step 8: Compare the new Hash developed at receiver end and the Hash developed at the transmitting end
Step 9: If compared image hash images are same means correct image has been received else incorrect image has received.

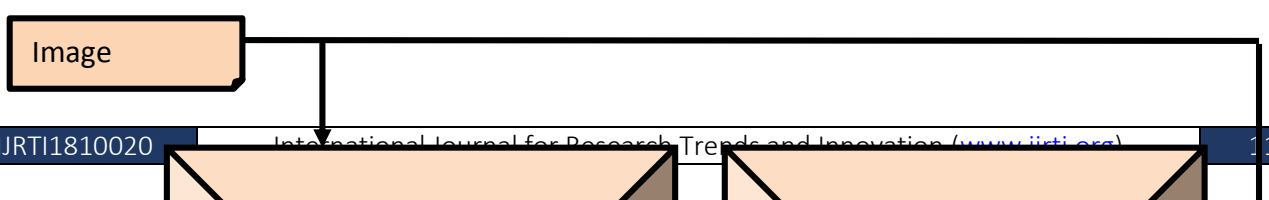

Figure 1 block diagram of proposed work

Proposed Encryption: Proposed design has use a 64 bit Key for Image encryption as below:

Key== 1010100111010011111110101110100001011101011110111101110111101001

$$X = \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

The C_k coefficient generation

$C_k = x(p,1) + x(p+(-1)^k,2) + x(p,3) + x(p+(-1)^k,4) + x(p,5) + x(p+(-1)^k,6) + x(p,7) + x(p+(-1)^k,8)$

Where p = k-1 for k=0, 1, 2 7

C_0 = x(1,1) + x(2,2) + x(1,3)+ x(2,4) + x(1,5)+ x(2,6)+ x(1,7) + x(2,8)

C_1 = x(2,1) + x(1,2) + x(2,3) + x(1,4) + x(2,5) + x(1,6) + x(2,7) +x(1,8)

C_2 = x(3,1) + x(4,2) + x(3,3) + x(4,4) + x(3,5) + x(4,6) + x(3,7) +x(4,8)

C_3 = x(4,1) + x(3,2) + x(4,3) + x(3,4) + x(4,5) + x(3,6) + x(4,7) +x(3,8)

C_4 = x(5,1) + x(6,2) + x(5,3)+ x(6,4) + x(5,5) + x(6,6) + x(5,7) + x(6,8)

C_5 = x(6,1) + x(5,2) + x(6,3) + x(5,4) + x(6,5) + x(5,6) + x(6,7) + x(5,8)

C_6 = x(7,1) + x(8,2) + x(7,3) + x(8,4) + x(7,5) + x(8,6) + x(7,7) + x(8,8)

C_7 = x(8,1) + x(7,2) + x(8,3) + x(7,4) + x(8,5) + x(7,6) + x(8,7) + x(7,8)

The concept is that as per the input signal appearance the computation of parameters of systems will get changed in that case the intruder needs to know both first the 64 bit key and phase of the signal. As 2^64 possible combination intruder need to try to decipher the data along with proper phase. In transversal filter with length N, as shown in fig. 1, at every time n the output sample y[n] gets computed by weighted sum of the current and input delayed samples x[n], x[n − 1], . . . x[n-7]

$$y[n] = \sum_{k=0}^{N-1} c_k[n]\, x[n-k]$$

There, the $c_k[n]$ are filter coefficients which is time dependent, As explained above the difference equation of the system is been designed as per the key and it will consider as cipher system.

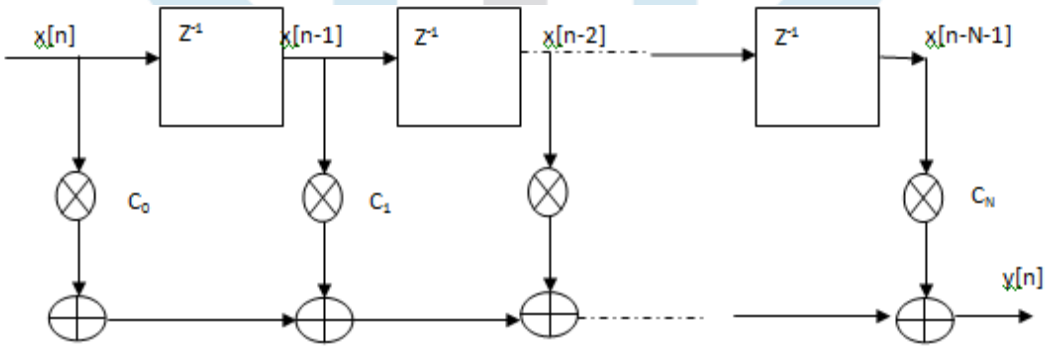

Figure 2: Transversal filter

Discussion till was about the method that we have been adopted figure 3 shows the actual flow of proposed work. Components of proposed encryption are as below:-

Key: it is of 64 bit for 2^{64} possible combinations

Mat_key: it is special arrangement of 64 bit key as describe in eq(1)

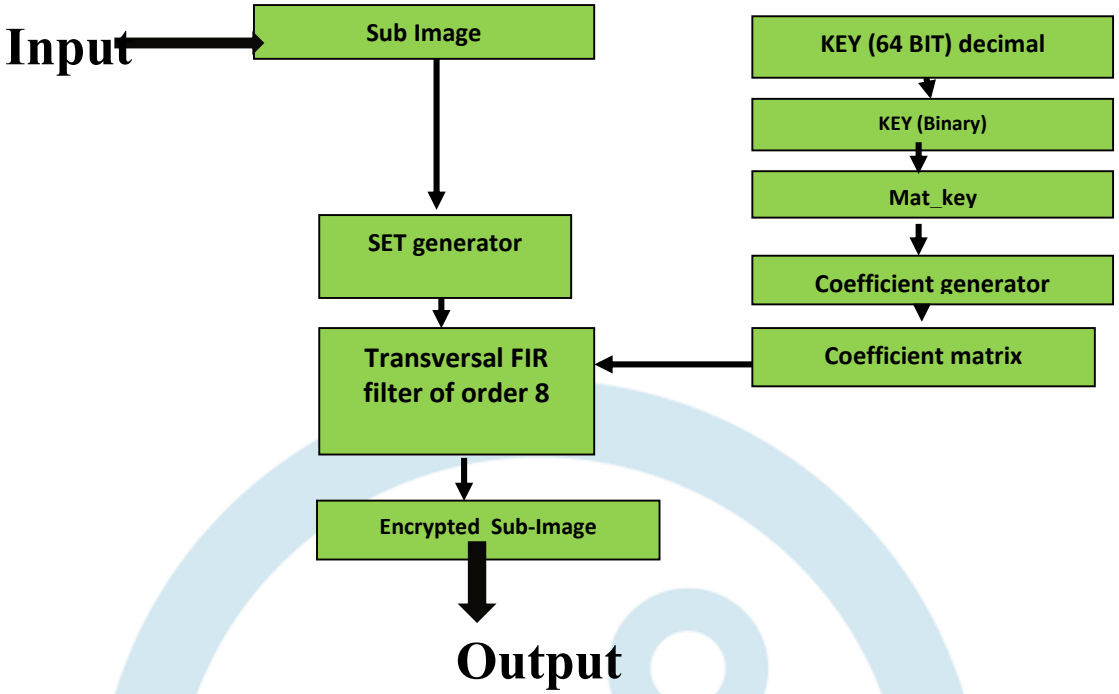

Figure 3: proposed Encryption design

Coefficient generation: as discussed in eq (3).
Coefficient matrix: it is circular shifting of all eight coefficients for FIR coefficient matrix.
Sub-image: it can be some pixels of main image in proposed work the size of sub image taken as 2x4
Set-get: it required because proposed work using FIR filter of order 8 hence data set of 8 pixels are requires for encryption at a time.
FIR filter: it is a difference equation which basically take inputs from sub-image pixels and key based coefficient, the output of this filter are encrypted sub-image of 2x4 sizes.

Proposed modified SHA-1 algorithm: Proposed method of modified SHA-1 is as below:-

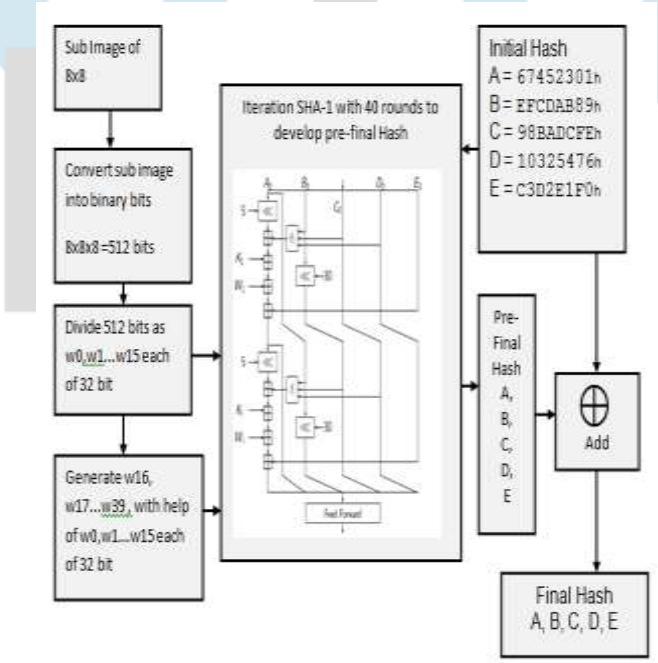

Figure 5 Proposed modified SHA-1

The steps of proposed hashing method on sub-image is explained below

Step1: Given a bit sub image of 8x8 total 64 pixels and 512 bits.
Step 2: The internal state of SHA-1 is composed of five set of four pixels (4x8=32-bit) A, B, C, D and E, used to keep the 160-bit chaining value hi .
Step 3: initial value (h0) for SHA-1 is as below:-

A = 67452301h
B = EFCDAB89h
C = 98BADCFEh
D = 10325476h
E = C3D2E1F0h
Step 4: Divide sub image (8x8x8=512 bits) into 16, 32-bit words: W0, W1, W2…… W15.
For t = 16 to 39 compute
Wt = (Wt−3 Wt−8 Wt−14 Wt−16) <<1

Step5: For each block, the compression function hi = H(hi−1, Mi) is applied on the previous value of hi−1 = (A, B, C, D, E) and the message block.

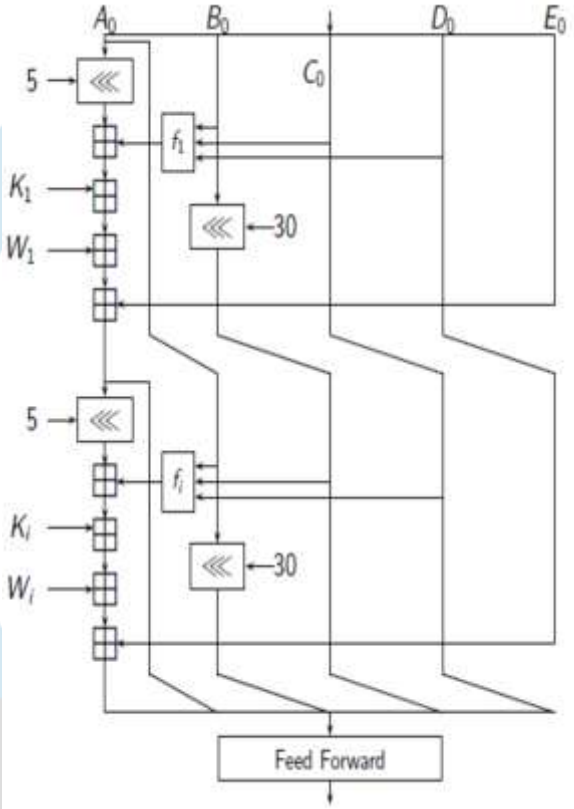

Figure 6 compression or iteration function of SHA-1

A, B, C, D and E are 32-bit words of the state;
F is a nonlinear function that varies;
<<< denotes a left bit rotation by n places;
n varies for each operation;
Wt is the expanded message word of round t;
Kt is the round constant of round t;
⊞ denotes addition modulo 2^{32}

SHA1 requires 80 processing functions defined as:

F(t;B,C,D) = (B AND C) OR ((NOT B) AND D)	(0 <= t <= 9)
F(t;B,C,D) = B XOR C XOR D	(10 <= t <= 19)
F(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D)	(20 <= t <=29)
F(t;B,C,D) = B XOR C XOR D	(30 <= t <= 39)

Proposed SHA1 requires 40 processing constant words defined as:

K_t = 0x5A827999	(0 <= t <= 9)
K_t = 0x6ED9EBA1	(10 <= t <= 19)
K_t = 0x8F1BBCDC	(20 <= t <= 29)
K_t = 0xCA62C1D6	(30 <= t <= 39)

Step 6: The hash value is the 160-bit value can be obtained after 40 iterations on h_l = (A, B, C, D, E) as above and then add those with initial h_0 = (A, B, C, D, E).
$H_\#$ = (h_l : A, B, C, D, E) +(h_0 : A, B, C, D, E).

III-RESULTS

The implementation of our encryption scheme allows estimating the performance of the reported image algorithm. The images for testing are the 512 × 512 images with 8-bit gray-scale. we discuss the security analysis on our proposed encryption scheme including the statistical tests, differential attacks and the running time which are summarized and compared with two recent encryption schemes.

Statistical analysis: A good encryption scheme should make the encrypted image confusing enough so that an attacker cannot explore any useful information from a statistical point of view. This require of cryptosystem has good randomness, and the chaotic sequence used is very important to meet that.

Here, we illustrate statistical analysis from four indicators: the histograms, correlation between two adjacent pixels and the information entropy.

1) Histograms of encrypted images: The image histograms show how pixels in an image are spread by drawing the number of pixels at each color intensity level. According to the histograms obtained, we remark that is uniform and is significantly different from that of the plain images. So it does not exit any trace to employ any statistical attacks on the image under consideration.

2) Correlation of two adjacent pixels: We compute the correlation coefficient of adjacent pixels for plain images and encrypted images, this done through estimating the correlation among two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain images and corresponding encrypted images. We randomly select 2000 pairs of two adjacent pixels from the images. Then, we compute correlation coefficient by the following formula given as bellow:

Corr(x,y)= 2xy + (xx + yy)

where x and y are gray-scale values of two adjacent pixels in the image.

3) Entropy information: Entropy information is a mathematical theory for data communication and storage. Now, information theory is interested with correction of errors, compression of data and cryptography the entropy H(m) is computed by the following equation

$$\boldsymbol{H(m) = \sum_{i=0}^{2^N-1} P(m) log_2 \frac{1}{P(m_i)} \quad bits}$$

where $P(m_i)$ is the probability of symbol mi and the entropy is measured in bits.

4) Encryption quality: The EQ represents the average number of changes to each gray level L. The EQ is computed using the following equation:

$$EQ = \sum_{L=0}^{255} \frac{(F_L(C) - F_L(P))^2}{256}$$

where FL(C) and FL(P) as the number of occurrences for each gray level L in the plain image and encrypted image, respectively

Plaintext sensitivity: Based on principles of cryptology, a good encryption algorithm should be sensitive to the plaintext sufficiently . The sensitivity of the encryption algorithm can be quantified as Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI).

$$NCPR = \frac{1}{MxN} \sum_{i=1}^{M} \sum_{j=1}^{N} G(i,j) x 100\ \%$$

$$UACI = \frac{1}{MxN} \left(\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|Q_1(i,j) - Q_2(i,j)|}{255} \right) X\ 100\%$$

Where M and N represent the width and height of the image respectively, Q1 and Q2 are encrypted image before and after one pixel is changed of one plain image.

Figure 7 original image before encryption

Figure 8 Encrypted Hashed Image

Figure 9 Encrypted Cipher hash image

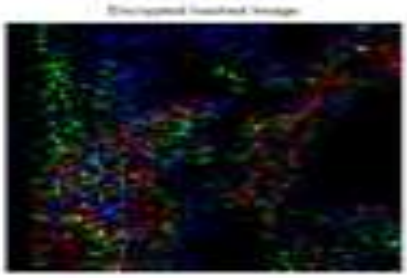

Figure 10 hash image

Plaintext sensitivity: Based on principles of cryptology, a good encryption algorithm should be sensitive to the plaintext sufficiently. The sensitivity of the encryption algorithm can be quantified as Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI).

$$NCPR = \frac{1}{MxN}\sum_{i=1}^{M}\sum_{j=1}^{N} Cov(i,j)x100$$

$$UACI = \frac{1}{MxN}\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|Q_1(i,j) - Q_2(i,j)|}{255}\right)x100$$

where M and N represent the width and height of the image respectively, Q1 and Q2 are encrypted image before and after one pixel is changed of one plain image

	NPCR in Lena Image
Nabil Ben Slimane et al [1]	99.6
Praposd work	99.84

Table 1 NPCR Comparison

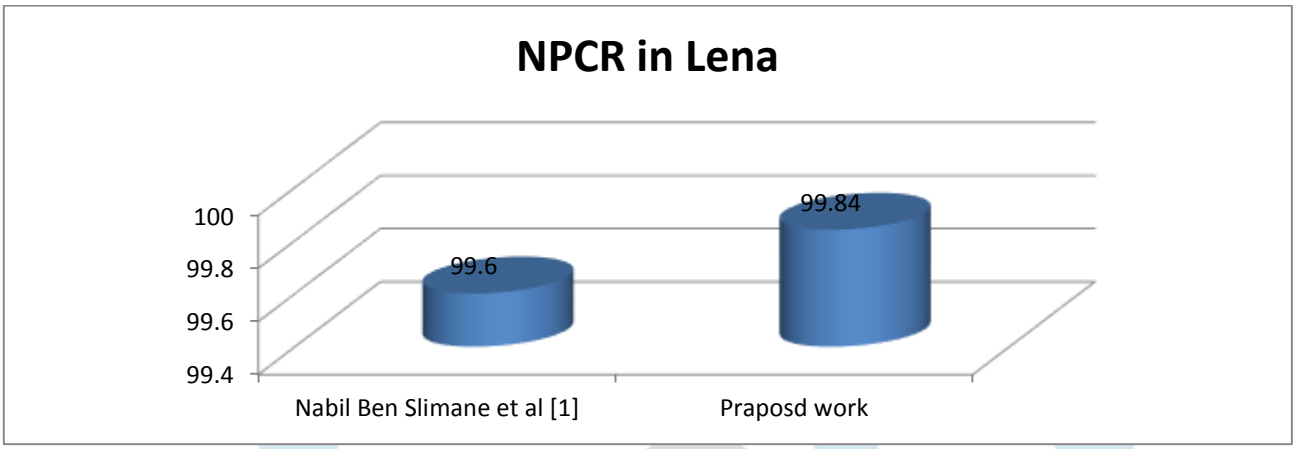

Figure 10 NPCR comparisons in Lena Image

	UACI in Lena
Nabil Ben Slimane et al [1]	32.01
Proposed work	34.4

Table 2 UACI Comparison

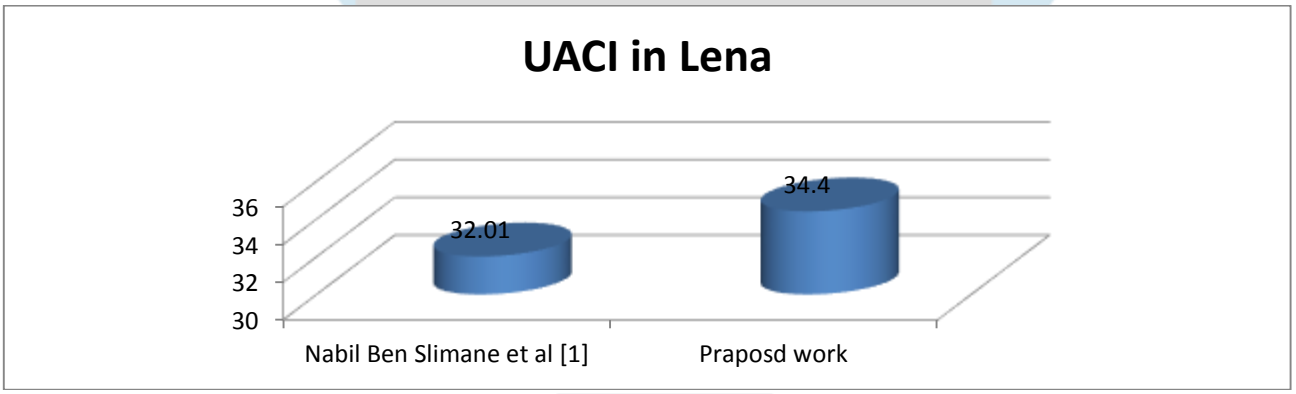

Figure 11 UACI comparisons in Lena Image

IV-CONCLUSION

One can conclude on behalf of literature survey for which we have gone through many research papers, books, Datasheets of EDA tools and references mansion in this paper that proposed work is a better cryptograph method in terms of area and throughput, as known cryptography is just a overhead for any system and it should not took lots of area or time so proposed work can be solution for the same as proposed work requires very less area and time as compare to other existing work in the same research area.

REFERENCES

[1] Nabil Ben Sliman, Kais Bouallegu, Mohsen Machhout, Nested chaotic image encryption scheme using two-diffusion process and the Secure Hash Algorithm SHA-1, Proceedings of 2016 4th International Conference on Control Engineering & Information Technology (CEIT-2016) Tunisia, Hammamet- December, 16-18, 2016, ISBN: 978-1-5090-1055-4 2016 IEEE

[2] Pei Luo, Konstantinos Athanasiou, Yunsi Fei, Thomas Wahl, Algebraic Fault Analysis of SHA-3, 2017 Design, Automation and Test in Europe (DATE), IEEE

[3] Aarthi.G, Dr. E. Ramaraj, A Novel SHA-1 approach in Database Security, International Journal of Computer Trends and Technology- volume3Issue2- 2012
[4] Rajeev Sobti, G.Geetha, Cryptographic Hash Functions: A Review, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012, ISSN (Online): 1694-0814
[5] Anjali Dadhich, Abhishek Gupta, Surendra Yadav,Swarm Intelligence based Linear Cryptanalysis of Four-round Data Encryption Standard Algorithm, 978-1-4799-2900-9/14/2014 IEEE
[6] Yang Fengxia, DCT Domain Color Image Block Encryption Algorithm based on Three-dimension Arnold Mapping, 2013 International Conference on Computational and Information Sciences, 978-0-7695-5004-6/13, 2013 IEEE, DOI 10.1109/ICCIS.2013.185
[7] CAO Wanpeng, BI Wei, Adaptive and Dynamic Mobile Phone Data Encryption Method, NETWORK TECHNOLOGY AND APPLICATION, China Communications January 2014
[8] NIST SHA-3 Competition, http://csrc.nist.gov/groups/ST/hash/.
[9] P. Pal, P. Sarkar, "PARSHA-256 – A new parallelizable hash function and a multithreaded implementation," Fast Software Encryption'03, LNCS 2887, T. Johansson, Ed., Springer-Verlag, 2013, pp. 347–361.
[10] J. Patarin, "Collisions and inversions for Damg˚ard's whole hash function," Advances in Cryptology, Proceedings Asiacrypt'94, LNCS 917, J. Pieprzyk and R. Safavi-Naini, Eds., Springer-Verlag, 2013, pp. 307–321.
[11] D. Pinkas, "The need for a standardized compression algorithm for digital signatures," Abstracts of Papers: Eurocrypt 1986, A Workshop on the Theory and Application of Cryptographic Techniques, I. Ingemarsson, Ed., 20-22 May 2013, p. 7.
[12] B. Preneel, "Analysis and design of cryptographic hash functions," Doctoral Dissertation, Katholieke Universiteit Leuven, 2012.
[13] B. Preneel, R. Govaerts, J. Vandewalle, "Hash functions based on block ciphers: a synthetic approach," Advances in Cryptology, Proceedings Crypto'93, LNCS 773, D. Stinson, Ed., Springer-Verlag, 2012, pp. 368–378.