A Review Study of Different Methods of Secure Hashing Algorithm using in Image Encryption Advantages

Ruchi Tiwari[1] Prof. Rajender Singh Yadav[2]
[1]M. Tech. Scholar [2]Professor
[1,2]GGITS, Jabalpur, India

Abstract— 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. 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

Cryptography is study & practice of techniques of secure data communication in presence of other parties. More details, it is about developing & analyzing protocols that avoid influence of adversaries & which are concern to various different aspects in information security such as data confidentiality, authentication, data integrity & non-repudiation. Now a day's cryptography intersects disciplines of computer science, mathematics & electrical engineering. Applications of cryptography include computer passwords, ATM cards & electronic commerce. The fig 1 shows a basic cryptographic model in which data which is to be transmitted is passed through encryption system & output so generated is called 'cipher'. On receiving terminal cipher is decrypted to get original data.

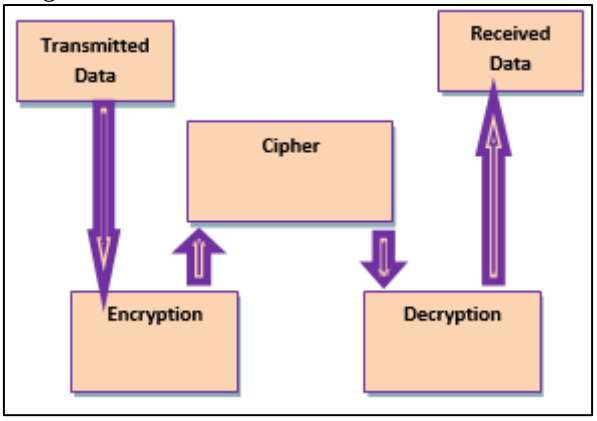

Fig. 1: Basic Encryption Model

Proposed working is using SHA-1 as hashing function. SHA isn't encryption, it's a one-way hash function. AES (Advanced_Encryption_Standard) is a symmetric encryption standard. SHA is a family of "Secure Hash Algorithms" that have been developed by the National Security Agency. There is currently a competition among dozens of options for who will become SHA-3, the new hash algorithm for 2012+. You use SHA functions to take a large document and compute a "digest" (also called "hash") of the input. It's important to realize that this is a one-way process. You can't take a digest and recover the original document. AES, the Advanced Encryption Standard is a symmetric block algorithm. This means that it takes 16 byte blocks and encrypts them. It is "symmetric" because the key allows for both encryption and decryption.

II. SECURE HASHING ALGORITHMS

Figure 2 shown below is showing basic concept of hashing it can be describe in following steps:-

1) Step 1: input the massage it can be a data or image
2) Step 2: perform encryption on massage using Key 'S'
3) Step 3: then perform Hashing method (H) on encrypted massage and develop Hash
4) Step 4: perform concatenation between original massage and Hash.
5) Step 5: At receiver end again perform encryption (with Key 'S') followed by Hashing (H) and develop new Hash
6) Step 6: now compare the hash which came along with the massage and the new hash which developed at receiving end.
7) Step 7: if matched then hashing correct else hashing with wrong massage.

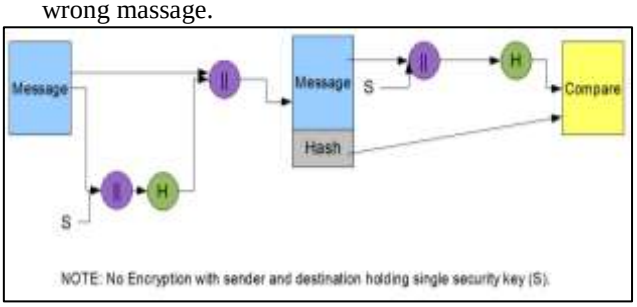

Fig. 2: Hashing fundamental concepts [3]

III. SHA-1 ALGORITHM

1) Step 1: Padding, Given an m-bit message, a single bit "1" is appended as the m + 1th bit and then (448 − (m + 1)) mod 512 (between 0 and 511) zero bits are appended. As a result, the message becomes 64-bit short of being a multiple of 512 bits long.
2) Step 2: Merkle-Damgard Strengthening or Append the length using A 64-bit representation of the original length of m is appended, making the result a multiple of 512 bits long.
3) Step 3: Division into Blocks The result is divided into 512-bit blocks, denoted by M1, M2, . . . , M_l.

4) Step 4: The internal state of SHA-1 is composed of five 32-bit words A, B, C, D and E, used to keep the 160-bit chaining value hi .
5) Step 5: Initialization: The initial value (h0) is (in hexadecimal)
   A = 67452301h
   B = EFCDAB89h
   C = 98BADCFEh
   D = 10325476h
   E = C3D2E1F0h
6) Step 6: Divide Mi into 16 32-bit words: W0, W1, W2, . . . , W15.
   For t = 16 to 79 compute
   Wt = (Wt−3 Wt−8 Wt−14 Wt−16) <<< 1.
   Remark the one-bit rotate in computing Wt was not included in SHA, and is the only difference between SHA and SHA-1.
7) Step 7: Compression: 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.

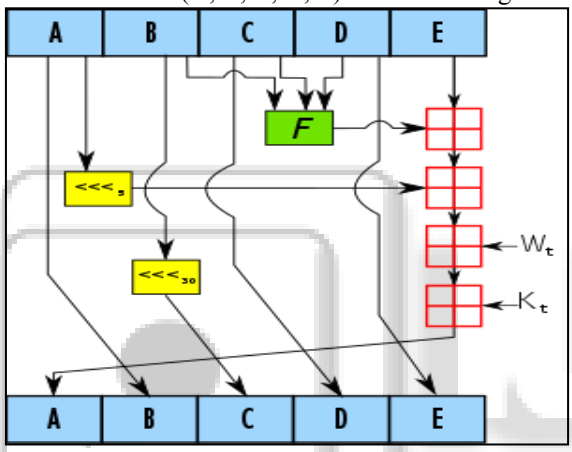

Fig. 3: compression or iteration function of SHA-1[1]

One iteration within the SHA-1 compression function:
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 <= 19)
F(t;B,C,D) = B XOR C XOR D
(20 <= t <= 39)
F(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D)
(40 <= t <=59)
F(t;B,C,D) = B XOR C XOR D
(60 <= t <= 79)
SHA1 requires 80 processing constant words defined as:
K_t = 0x5A827999 (0 <= t <= 19)
K_t = 0x6ED9EBA1 (20 <= t <= 39)
K_t = 0x8F1BBCDC (40 <= t <= 59)
K_t = 0xCA62C1D6 (60 <= t <= 79)
Step 8: The hash value is the 160-bit value can be obtained after 80 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).

IV. REVIEW OF AVAILABLE WORK

Cryptographic hash functions map input strings of arbitrary (or very large) length to short fixed length output strings. In their 1976 seminal paper on publickey cryptography, Diffie and Hellman identified the need for a one-way hash function as a building block of a digital signature scheme. The first definitions, analysis and constructions for cryptographic hash functions can be found in the work of Rabin , Yuval , and Merkle of the late 1970s. Rabin proposed a design with a 64-bit result based on the block cipher DES , Yuval showed how to find collisions for an n-bit hash function in time 2n/2 with the birthday paradox, and Merkle's work introduced the requirements of collision resistance, second preimage resistance, and preimage resistance. In 1987, Damg˚ard formalized the definition of collision resistance, and two years later Naor and Yung defined a variant of seoncd preimage resistant functions called Universal One Way Hash Functions (UOWHFs) (also known as functions 2 B. Preneel offering eSEC). In 2004 Rogaway and Shrimpton formally studied the relations between collision resistance and several flavors of preimage resistance and second preimage resistance. Hash functions should also destroy the algebraic structure of the signature scheme; typical examples are the Fiat-Shamir heuristic and Coppersmith's attack on the hash function in X.509 Annex D that was intended for use with RSA [7] (this attack breaks the signature scheme by constructing message pairs (x, x0) for which h(x) = 256 · h(x 0)). This development resulted in the requirement that hash functions need an 'ideal' behavior which would allow them to instantiate the theoretical concept of random oracles (see e.g. Bellare and Rogaway). Constructions of MAC algorithms based on hash functions (such as HMAC) have resulted in the requirement that the hash function can be used to construct pseudo-random functions, which has a.o. been studied by Bellare et al.

Abhilash Ashok Bhadke et al [1] they propose an encryption technique for images which is hybrid of Lorentz attractor and Secure Hash Algorithm (SHA-2) applied on separated bit planes of the image. Their research utilize the chaotic nature of the Lorenz attractor and has significantly improved the entropy, which is an important parameter to measure the randomness. They also introduce a new method of implementing chaotic scheme. SHA-2 and Lorentz attractor are used to generate the key matrix. Bit-plane slicing is carried out on the plain image to decompose it to 1-D data and then X-OR operation with the key matrix is performed. The encrypted file is subjected to various analysis and attacks. The results demonstrate that the algorithm is resistant to various known attacks along with desirable security performance. Both encryption and decryption in the proposed algorithm are loss less. Nabil Ben Slimane et al [2] In this work, an efficient, secure and robust scheme for image encryption is reported which is realized using two main diffusion stages based on nested chaotic attractor and the Secure Hash Algorithm SHA-1. Each diffusion stage use a special component of nested chaotic sequence combined with chaotic attractor of Chua to modify the values of image pixels and encrypt the plain image. According to the illustrated

results, our image encryption scheme has a good cryptographic features in level security and speed for image encryption.

Pei Luo et al [3] presents an efficient algebraic fault analysis on all four modes of SHA-3 under relaxed fault models. This is the first work to apply algebraic techniques on fault analysis of SHA-3. Results show that algebraic fault analysis on SHA-3 is very efficient and effective due to the clear algebraic properties of Keccak operations. Comparing with previous work on differential fault analysis of SHA-3, algebraic fault analysis can identify the injected faults with much higher rates, and recover an entire internal state of the penultimate round with much fewer fault injections. Aarthi.G et al [4] proposed technique is going to design the database encryption with high performance. Database encryption is being shown as the strongest security alternative for the data protection. The main objective of thispaper is to give data security protection at data rest in database. Rajeev Sobti et al [4] bring out the importance of hash functions, its various structures, design techniques, attacks and the progressive recent development in this field.

Author	Journal	Title	Work	Outcome
Rajeev Sobti et al [5]	IJCSI, 2012	Cryptographic Hash Functions: A Review	importance of hash functions, its various structures, design techniques, attacks	--
Aarthi.G et al [4]	IJCTT 2012	A Novel SHA-1 approach in Database Security	Single field that is act as primary part of the row or column, they also use SHA-1 using DBMS and storing the hashing coefficients not generating that.	--
Pei Luo et al [3]	IEEE. 2017	Algebraic Fault Analysis of SHA-3	Apply algebraic techniques on fault analysis of SHA-3. Algebraic fault analysis can identify the injected faults with much higher rates, and recover an entire internal state of the penultimate round with much fewer fault injections.	Effective fault ratio 96.85% for 246 bit SHA3 using their algebraic fault analysis (AFA) method
Nabil Ben Slimane et al [2]	IEEE 2016	Nested chaotic image encryption scheme using two-diffusion process and the Secure Hash Algorithm SHA-1	Propose a fast, secure and light weight scheme for digital image encryption based on nested chaotic attractors using the Secure Hash Algorithm SHA-1 using only two-diffusion process	Number of Pixels Change Rate (NPCR) 99.60. Unified Average Changing Intensity (UACI) 32.01
Abhilash Ashok Bhadke et al [1]	IEEE 2018	Symmetric Chaos Based Image Encryption Technique on Image Bit-Planes using SHA-256	Propose an encryption technique for images which is hybrid of Lorentz attractor and Secure Hash Algorithm (SHA-2) applied on separated bit planes of the image. their research utilize the chaotic nature of the Lorenz attractor and has significantly improved the entropy, which is an important parameter to measure the randomness.	for Lena image NPCR observe is 99.609 UACI Observe is 33.42 and Entropy 7.9998.

Table 1: Literature work Review

Cryptography is method for secure data and because of intruders it as became essential and some time it is very complex so it requires very high computation and huge area requirement and also need lots of time to generate the hash function which overall reduce the throughput, The available Encryption methods like DSA, MD4, MD$, SHA-1, SHA-2 and SHA-256 etc. are good enough but require lots of time and area and power requirement like for this a new hashing method is been developed and presented in the thesis work which is highly secure (highly avalanche), highly throughput as compare existing encryption methods.

Rajeev Sobti et al [4] just represent a review work of hashing methods, Aarthi.G et al [3] represent a new work for hashing in which they use DBMS for hashing which consume a string type data structure at the system and hence need lots of memory. Pei Luo et al [2] develops SHA-3 under relaxed fault models in which they develop a new algebraic method to identifies the injected faults or attacks in hashing method but the algebraic computation requires equal time as was required in hashing which make their method slower also they use SHA-3, proposed work is using SHA-1, SHA-3 is a advance variant of SHA-1 but less popular because less advantage over SHA-1 and more computation requirements. Nabil Ben Slimane et al [1] develop scheme for digital image encryption based on nested chaotic attractors using the Secure Hash Algorithm SHA-1, they develop a Nested chaotic attractor which is a add-on in available SHA-1 method and that reduces the speed. Because they are using their nested chaotic attractor at each SHA-1 iteration and there are total 80 iteration means there method will execute total 80 times and that will take lots of time in image processing.

The main aim of proposed work is to design, simulate and verify the functionality of proposed hashing method which is highly computationally expensive and are highly challenging in other available methods. To develop proposed work as a free module in a high speed secure network. This can be said in elaborated as: When confidentiality concerns, the motive is to design an optimized architecture for hashing which is highly complex with very less area and time requirement.

V. CONCLUSION

As known cryptography is just a overhead for any system and it should not took lots of time so proposed work is a solution for the same as proposed requires very less time and highly security (i.e. high avalanche effect) as compare to other existing work in the same category. One can conclude that the SHA encryption method has fastest among the available methods like AES, DES and RSA. The SHA technique is also faster than method developed by researchers of [6],[5] and [9]. The total avalanche observed for SHA technique is 76% which is best among the all method available hence SHA work is a better cryptograph method in terms of throughput and security level. In future the steganography algorithms can be added to SHA method to improve the capacity of the cryptography process. In the case of cryptography, some more complex algorithms can be used then proposed FIR filter difference equation module, but the data usage, hardware implementation processing time and other factors should be taken into account.

REFERENCES

[1] Abhilash Ashok Bhadke, Surender Kannaiyan, Vipin Kamble, Symmetric Chaos-Based Image Encryption Technique on Image Bit-Planes using SHA-256, 2018 Twenty Fourth National Conference on Communications (NCC), ISBN: 978-1-5386-1224-8/2018, IEEE
[2] 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
[3] Pei Luo, Konstantinos Athanasiou, Yunsi Fei, Thomas Wahl, Algebraic Fault Analysis of SHA-3, 2017 Design, Automation and Test in Europe (DATE), IEEE
[4] Aarthi.G, Dr. E. Ramaraj, A Novel SHA-1 approach in Database Security, International Journal of Computer Trends and Technology- volume3Issue2- 2012
[5] 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
[6] 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
[7] 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
[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. 7-13.
[12] CAO Wanpeng, BI Wei, Adaptive and Dynamic Mobile Phone Data Encryption Method, NETWORK TECHNOLOGY AND APPLICATION, China Communications January 2014

