2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)
IMS Engineering College, Ghaziabad, India

Digital Image Authentication and Encryption using Digital Signature

Shahzad Alam, Amir Jamil
Department of Computer Engineering,
Faculty of Engineering and Technology,
Jamia Millia Islamia, New Delhi-110025, India
{shazad5alam, amirjamil900}@gmail.com

Ankur Saldhi, Musheer Ahmad
Department of Computer Engineering,
Faculty of Engineering and Technology,
Jamia Millia Islamia, New Delhi-110025, India
{ankur479225, musheer.cse}@gmail.com

***Abstract*—In this paper, a methodology for digital image authentication using digital signature is proposed. The hash of the original image is taken and is encrypted by RSA. The digital signature obtained is concealed in the image. Digital signature is sent along with the encrypted image which decreases the probability of meticulous attack by the intruder. The encrypted image is shuffled using Chaotic Logistic Map to get the final shuffled encrypted image. The use of Logistic Map improves the randomness in the image. For the authentication, a comparator is employed which evaluates correctness of the hash extracted. The simulations have been carried out to examine the proposed authentication and encryption technique.**

Keywords—Digital signature, reed solomon encoding, logistic map, RSA, SHA-1 .

I. INTRODUCTION

In modern era, technology has its own benefits and pitfalls. The major drawbacks include the unethical intrusion over the channels to steal the important information from the sender. To reduce the information leakage over the channels, various encryption methods [13, 14] have been proposed. With the advancement in technology, the security of digital images has become more and more crucial since the communications of digital products over internet are taking place more and more frequently. The organizations are migrating towards the electronic documents to reduce the paper work. To safeguard the electronic documents from potential hackers, public-key cryptography [1, 3, 6] known as digital signatures are used to authenticate the data sent over the channels. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and protection in transmission of information in digital form [9]. Encryption can protect the privacy of data, but other methods are still needed to protect the integrity and authenticity of data. For example verification of a message authentication codes (MAC) or a digital signature. A digital signature [7] has many advantages like relative alleviate of laying down that the signature is authentic, the difficulty of forging a signature, the non-transferability of signature, the difficulty of altering signature, and the nonrepudiation of digital signature to insure that the signer cannot later deny signing. The signature must employ some information which is unique to sender to preclude both counterfeit and denial [8]. It must be comparatively easy to produce. To tackle this problem, a simple and effective method employing the concept of digital signature and error coding technique for image encryption is proposed by Aloka [1]. In Aloka *et al.* the digital signature is appended to the encoded image which is obtained by applying BCH encoding technique. At the receiver side, the digital signature can be employed to verify the legitimacy of the image. A digital correlation technique is used to verify the legitimacy of the deciphered image. In this paper, we tapped the features of SHA-1 hash scheme, Reed Solomon algorithm and digital signature to verify the authenticity of the image received. We used chaotic logistic map to spread the digital signature within the encrypted image, consequently making the proposed technique secure.

II. PRELIMINARIES

In this section, we discuss the prerequisite which are required in the proposed approach. SHA-1, Reed Solomon code, RSA and Logistic map are briefly described below:

A. SHA-1 hash generation

SHA1 is an acronym for "Secure Hashing Algorithm". It is a hash algorithm designed by the US National Security Agency and released by NIST. It is better than the previous SHA-0 algorithm and was first published in 1995. SHA-1 is presently the most widely used SHA [11] hash function. SHA-1 produces the outputs of 160-bit digest of all sized file or input. In implementation, it is like to the former MD4 and MD5 hash functions, in fact dealing some of the initial hash values. It employ a 512-bit chunk size and has a content size of 2^{64}- 1 bits. As an example, the message "*hello word*" has a hash value given by:

"*aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d*".

978-1-4673-6911-4/15/$31.00©2015 IEEE

B. Reed Solomon Algorithm

Reed-Solomon codes are block-based codes having a wide range of applications in digital transmission and storage of digital data. The Reed-Solomon encoder takes a chunk of digital information and adds additional "supernumerary " bits in the information as shown in Figure 1. Errors occur during communication or storage of bits for a number of causes. The Reed-Solomon decoder processes each chunk (block) and then tries to rectify errors and retrieve the original information. Reed Solomon codes are linear block code and sub set of BCH codes. RS (n, k) with s-bit symbols indicates that the encoder takes k bits of information symbols of s bits each and adds extra redundant parity bits to construct an n bits of symbol code word.

There are n and k extra redundant symbols of each s bits. A Reed-Solomon decoder can rectify up to t bits that incorporate errors in a code word, where 2t = n-k. Following diagram shows a typical format of Reed-Solomon codeword.

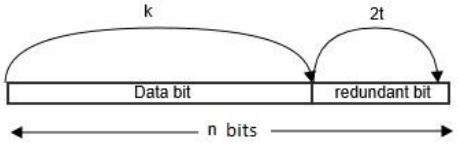


Fig. 1. Reed-Solomon code word

A popular Reed-Solomon code is RS (255, 223) having 8-bits of symbols. Each code word comprises 255 code word bytes in which 32 bytes are extra redundant parity bits and 223 bytes are information and. An Example can be taken into consideration:

$$n = 255, k = 223, s = 8$$
$$2t = 32, t = 16$$

The decipherer can rectify up to 16 symbol faults anywhere in the code word and can be automatically rectify the errors. Given a symbol size of s bits, the upper bound of word size (n) for a Reed-Solomon code is given by:

$$n = 2^s - 1.$$

C. RSA

RSA is public-key cryptosystems and is widely applied for safe information transmission. It is an asymmetric cryptographic algorithm. RSA is an acronym for Ron Rivest, Adi Shamir and Leonard Adleman, who formulated encryption algorithm in 1978. It involves a public key and private key. In RSA, both the public and the private keys collectively encrypt the plaintext message; the opposite key from the one used to encrypt a message is used to decrypt it. It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

D. Chaotic Logistic Map

The one-dimensional Logistic map proposed by R. M. May [12] is one of the simplest nonlinear chaotic discrete systems that show disorderly behavior; it is governed by the following equation.

$$z(n+1) = \lambda \times z(n) \times (1 - z(n)) \quad (1)$$

Where z is map's variable and z(0) acts as the initial condition, λ is system parameter and n is number of iterations needs to be applied. The research shows that the map exhibits chaotic dynamics for $3.57 < \lambda < 4$ and $z(n) \in (0, 1)$ for all n. This chaotic map is used to select 1-D matrix values in random fashion.

III. Proposed Algorithm

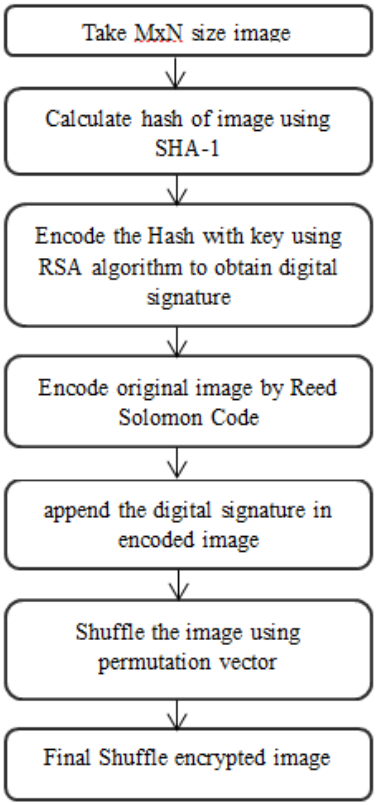
In this section, we propose our method. The SHA-1, Reed Solomon Algorithm, RSA and logistic map are employed in the proposed design methodology.

Firstly, we generate a hash of the image using SHA-1 technique and apply RSA on the hash to obtained digital signature. This is done for checking the authenticity of image at the receiver end. Apply the Reed Solomon Encoding Algorithm on image to add redundant data that encodes the image. Then append the digital signature in it to obtain an encrypted image. Finally shuffle the image using permutation vector with the help of 1D logistic mapping [12] technique to get the final encoded image. At the receiver end reverse process is applied to check the authenticity of image. A valid digital signature gives a receiver a reason to confident that the encoded image was produced by a known sender and that the image was not altered in transit (integrity). Even if the image is intruded at the receiver end, the receiver will be able to differentiate between obtained image and original image by comparing their hashes respectively. The flow chart and block diagram explains the process of proposed encryption algorithm shown in figure 2. The steps of proposed image encryption algorithm are as follows:

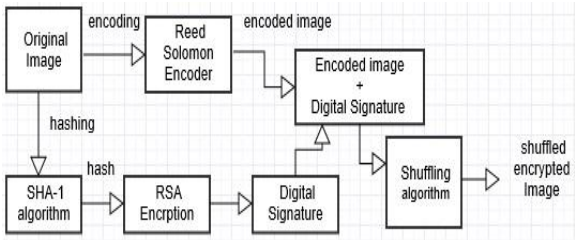
A.1. A plain image M*N dimension is taken.
A.2. Take out the hash of the image using SHA-1
A.3. Apply RSA algorithm to encrypt the hash with a private key. We get the 64 byte digital signature as a result.
A.4. Apply Reed Solomon Encoding algorithm on original image
A.5. Append the digital signature with the encoded image to get the encrypted image.
Encrypted image =append (encoded image + digital signature)
A.6. The encrypted image is shuffled using chaotic Logistic mapping.
A.7. resultant encrypted image

The decryption process is similar to the encryption process but all the operations are applied in reverse order. The hash values are compared at the end. If they are equal then image is authenticated otherwise image is intruded in while transmission on the network. The steps of image decryption algorithm are as follows:

B.1. Use the reverse shuffling algorithm to deshuffle the encrypted image.
B.2. Get a deshuffled image .Now separate the digital signature and the encoded image.
B.3. The encoded image obtained is decoded using Reed Solomon Decoder and finally the original image is obtained.
B.4. Next we decrypt the digital signature which is sliced from encrypted image, using public key RSA .We get the hash value.
B.5. Finally take out the hash of obtained image (final) using SHA-1. Compare the hashes of obtained image (final) and one obtained in step B4.
B.6. If the hashes are same, then there is no noise interruption. Else if hashes are not same then there are some bits changes made by the intruder.



(a)



(b)

Fig. 2. (a) Encryption process and (b) Block diagram of encryption process

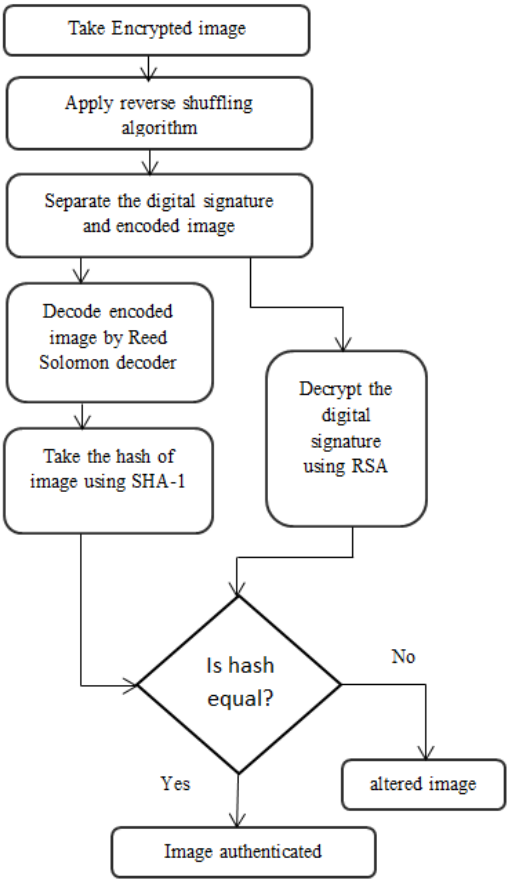


Fig. 3. Decryption process

IV. SIMULATION

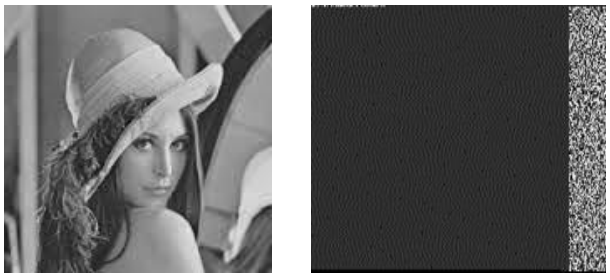
This section presents experimental results for Lena image. The proposed scheme is simulated on Python language to verify the correctness of the proposed methodology for image encryption. The figure 4 and figure5 shows the simulation result on gray scale Lena. The original image is encoded using RS algorithm before the addition of digital signature. The message digest generated by using SHA-1 and encrypted by RSA

algorithm to obtain 64byte or 512bit as shown in table 1. The encrypted image obtained is larger in size than the original Lena image because of redundant bits added due to error control coding.

At the receiver side decision is taken after obtaining the hash value of image and embedded hash value. If the hash values are same then this is the indication that the original image has not been intervened by intruders. If image is altered as shown in figure 4(e) then it is easily detected by comparing the hash values. This enables us to authenticate the image transmitted by the known sender. The added advantage in proposed technique is that there is no requirement to transmit separately the random keys.

TABLE I. SIMULATION RESULTS FOR LENA IMAGES

	Image	**Generated Hash**	**Decision (Authentic?)**
Sender Side	Lena image 1 (Fig. 4a)	d2d6ea25b078a115 bb4f89e24df6c ba0c770977c	--
Receiver Side	Lena image 2 (Fig. 5b)	d2d6ea25b078a115 bb4f89e24df6c ba0c770977c	Yes (No intrusion detected)
Receiver Side	Altered Lena image 3 (Fig. 5c)	cbdeb3c2adb63c4 7412f0644421ac7 a7bb1feb44	NO (intrusion detected)



(a) (b)

Fig. 4: (a) Original Lena Image 1 (b) Encoded Image

(a) (b)

(c)

Fig. 5. (a) Encrypted image and (b) Recovered Lena Image 2 and (c) Altered Lena Image 3

IV. CONCLUSION

The robust technique of image authentication and Image encryption technique based on digital signature and error correcting code is proposed. It has implemented successfully in Python language. We have tested the algorithm on the Lena image. The dimension of image is changed due to addition of extra bits by Reed Solomon code that makes difficulty to encrypt the image. The authenticity of received image is checked using digital signature. This project successfully transfers the digital signature over the channel without giving the chances of intrusion by the intruder. Even if the image is intruded at the receiver end, the receiver will be able to differentiate between obtained image and original image by comparing the hashes. The digital signature is also verified with the same technique. Furthermore, the algorithm is shown to be highly sensitive to its alteration of image. Experimental results show that our scheme has high security and is capable of authenticating the image.

To employ a more secure image encryption, X-box Mapping may be used which uses no stego keys, on which we will lay emphasis in our future works.

REFERENCES

[1] A. Sinha, K. Singh, “A technique for image encryption using digital signature”, Optics Communications, vol. 218, no. 4-6, pp. 229–234, 2003.

[2] Nidhi Sethi,Deepika Sharma “A novel method of image encryption using logistic mapping”, International Journal of Computer Science Engineering, vol. 01, no. 2, pp. 115-119, 2012.

[3] B. Schneier, “Applied cryptography algorithms”, Wiley, 1996.

[4] R. Blahut, “Theory and practice of error control codes”, Addison Wesley, Reading, MA, 1983

[5] F. MacWilliams, N. Sloane, “The theory of error correcting codes”, North Holland, Amsterdam, 1977.

[6] H. Feistel, "Cryptography and computer privacy", Scientific American, vol. 228, no. 5, pp. 15-23, 1973.

[7] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM vol. 21, no. 2, pp. 120–126, 1978.

[8] D. Bhattacharya, N. Bansal, A. Banaerji and D. R. Chowdhury, "A near optimal S-box design", Information Systems Security, Lecture Notes in Computer Science, vol. 4812, pp. 77–90, 2007.

[9] S. Alam, S. M. Zakariya, and Nadeem Akhtar, "Analysis of modified Triple-A steganography technique using Fisher Yates algorithm", International Conference on Hybrid Intelligent Systems , doi: 978-1-4799-7633-1/14/ 2014.

[10] FIPS 180-3, Secure Hash Standard - National Institute of Standards and Technology: http://csrc.nist.gov/publications/fips/fips1803/fips1803_final.pdf

[11] SHA-1: http://en.wikipedia.org/wiki/SHA1

[12] R. M. May, "Simple mathematical model with very complicated dynamics", Nature, vol. 261, pp. 459–467, 1967.

[13] M. Ahmad and O. Farooq, "Chaos based PN sequence generator for cryptographic applications", International Conference on Multimedia, Signal Processing and Communication Technologies, pp. 83-86, 2011.

[14] M. Ahmad and O. Farooq, "Secure satellite images transmission scheme based on chaos and discrete wavelet transform", In: Mantri, A., Nandi, S., Kumar, G., Kumar, S. (eds.) HPAGC 2011. CCIS, vol. 169, pp. 257–264. 2011.