Concealment of Data with MSB using Modified Secure Hash Algorithm

P. Srividdhya[1]
Department of Electronics and Comunication Engineering,
Sri ManakulaVinayagar Engineering College,
Madagadipet, Puducherry-605107, India

K. Dhanasekaran[2]
Department of Electronics and Comunication Engineering,
Mailam Engineering College,
Mailam, Villupuram-604304, Tamil Nadu, India

Abstract **- Data concealment is additionally necessary as a result of the key message that will share solely concealment of the info with image, audio, or video signal. The hacker will simply attack the message and take the key message. Therefore additional powerful concealment methodology and rule square measure needed. During this paper, we tend to discuss like that one amongst the rule. Modified secure hash algorithm that is that the advanced version of a message digest and secure hash function and conjointly exploitation the most significant bits (MSB) for knowledge concealment. Principally hackers attack solely Least significant Bits(LSB) simply however attack of MSB many times its injury the total message. Therefore finally concealment the info in MSB with modified hash algorithm results shows that not solely can do smart results and conjointly excellent concealment ability from completely different attacks with effective output.**

Keywords - Data concealment, Modified secure hash algorithm, Most significant bits (MSB), Least Significant Bits (LSB), Message digest, attack, hacker

I. INTRODUCTION

Due to usage of network is quickly magnified now-a-days, that the security of knowledge is a lot of necessary. We have a tendency to area unit having a lot of algorithms however there's less security and hacker will simple determine the key[1]. Some rules have a lot of advanced to style thus principally user prefers the algorithm that is less difficult and economical.

In this paper the most aim is to style associate degree rule that is a lot of economical to cover the information and receiver will receive the key message while not corrupted. Equally we are able to use the methodology to cover the information in most significant bits (MSB). As a result of most of the activity techniques used LSB techniques to cover the key message thus hackers simply hack the LSB term. However we are able to hide the information in most significant bits (MSB) it’s robust to spot the message[1].
The secret message is activity with most significant bits (MSB) and cypher to image. That stego image is send to receiver wherever the image is decoded with the changed secure hash rule[2]. This rule will turn out the output as 1024 bits with a block size of 576 bits. By adding a lot of pictures will offer extra security to send the photographs[3].

It is a way to modulate a message within a medium of misunderstanding specified the existence of the message is each hidden and troublesome to recover once discovered[4]. Several algorithms and procedures, like Least Significant Bit (LSB), are written to cover text in a picture[5][6]. The goal is to create communication unintelligible to those that don't possess the correct keys.

II. HIDING INFORMATION IN MOST IMPORTANT BYTE

In computing, the foremost vital bit is that the bit position in an exceedingly binary variety having the best worth. The most significant bits (MSB) is typically spoken because the high-order bit or left-most bit because of the convention in system of numeration of writing a lot of vital digits any to the left[10].

The most significant bits (MSB) may correspond to the sign little bit of a signed binary variety. In one's and two's complement notation, "1" signifies a negative variety and "0" signifies a positive variety[7].

It is common to assign every bit a grip variety starting from zero to N−1 wherever N is that the variety of bits within the binary illustration used. Normally, this is often merely the exponent for the corresponding bit weight in base-2. Though many CPU makers assign bit numbers the other means, the most significant bits (MSB) unambiguously remains the foremost vital bit. this might be one in every of the explanations why the term most significant bits (MSB) is usually used rather than a small amount variety, though the first reason is perhaps that completely different variety representations use different numbers of bits[6].

By extension, the foremost vital bits area unit the bits nearest to, and as well as, the MSB. The expressions most vital important bit initial and least significant bit initial area unit indications on the ordering of the sequence of the bits within the bytes sent over a wire in an exceedingly transmission protocol or in an exceedingly stream.

Most vital bit initial implies that the foremost significant bit can arrive first: thence e.g. the positional notation variety 0x12, 00010010 in binary illustration, can arrive because the sequence 00010010.

Least vital bit initial implies that the smallest amount vital bit can arrive first: thence e.g. an equivalent positional notation variety 0x12, once more 00010010 in binary illustration, can arrive because the sequence 01001000.

The below is mentioned the cryptography in most significant bits (MSB) term, wherever the message bit is 01101100 and therefore the secret message is 00110011. the key message is cypher with the most significant bits (MSB) term and obtained as a price of 00111100.

First four bits denotes the worth of secret codes and LSB is denotes the message bit value.

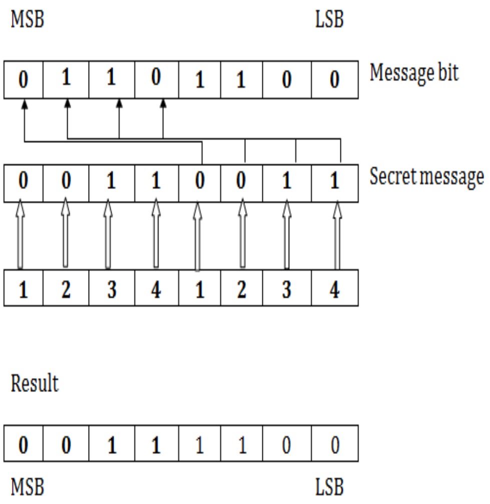

Fig.1. Encoding the secret message with MSB

III. MODIFIED SECURE HASH ALGORITHM

In the existing system LSB methodology begin by passing each secret message and canopy image into the encoder. Then within the encoder, one or many protocols are going to be enforced to imbed the key data into the quilt medium to supply another seem like copy of the first covering medium that it'll be referred to as stegoimage. A key's required within the embedding method. Key may be wont to scale back the possibility of third party attackers obtaining hold of the stegoimage and secret writing it to search out out the key data.

Hash rule is associate degree rule to secure the information with key. The classification of SHA (secure hash algorithm) could also be rely on security against collision attacks in bits. MD5 is associate degree rule that is simple to cover the information wherever its method but <18 collisions found. equally SHA-0, SHA-1, SHA-2, and SHA-3 wherever its method <34 collisions, <63 collisions and 112, 128 and 256 collisions attacks.

Our changed rule have the collision attacks has 256 bits. The entire rule may be processed with the LSB collision attacks however our rule may be exhausted most significant bits (MSB) that the capability of its extension attacks is 1024 bits. Changed secure hash rule is processed with key to cypher the information to cover within the image. Receiver additionally would like the key to rewrite the information.

Mostly hacker will decide to hack the key and rewrite the information in image. From purpose of hacker a lot of existing methodology won't to method with LSB so that they will target to rewrite the terms in LSB solely and procure wrong information. Whereas activity the information in most significant bits (MSB), it's not possible to search out the information and additionally mix with secure rule its create robust work to hack.

One is cypher the information with key and another one is while not key. If our rule cypher the information with key and at that very same time the key additionally send to the actual receiver with order format. Thus while not data of sender nobody will rewrite the information even a receiver additionally.

Consider the color image that its pixel worth is represent as R=10110111, G=10010100, B=11001001, and therefore the secret information that is cypher with the color image is 1001001, now apply the hash operate in most significant bits (MSB) term of color pictures and therefore additionally the position also determined.

The position of R=1,2,3, G=4,1,2 and B=3,4. that the secret message cypher with position of pixel and procure the result as R=10010111, G=00010100, B=1001001.

IV. ENCODING PROCESS

Encoding is that the method of activity the information to audio, image or video with appropriate rule. during this section the cryptography method area unit consult with step by step

Step 1: Secret message is method with SHA rule with public key and cipher text area unit shaped. Cipher text could be a cryptography format of knowledge with rule.

Step 2: Choosen a cowl image. wherever cowl image is black and white suggests that it's a lot of economical to cover the information. as a result of compare with color image black and white image carries with it less pixel with high intensity. thus information may be simply mapped with it.

Step 3: Produce a stego image. Merge the quilt image and cipher text is termed stego image. When the creation the stego image solely cryptography method is completed .

Step 4: the stego image is send to receiver. This stego image carries with it image and secret text. With the proper data of receiver solely this stego image may be transmitted to receiver.

Depend upon the rule the cryptography is a lot of economical, compare with the LSB process the mixture of most significant bits (MSB) with hash functioning is a lot of power rule to cypher the information with secure.

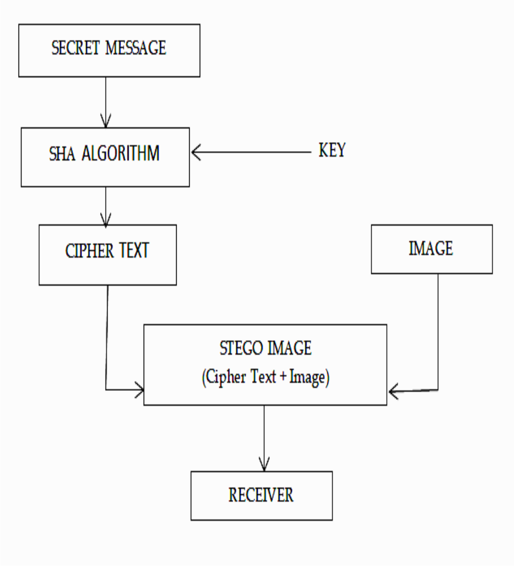

Fig.2. Creation of Stego Image

V. DECODING PROCESS

It is a method of decide the hide text within the given image.the step of secret writing is describe one by one

Step 1: Stego image is receive by receiver

Step 2:Decode the stego image and split one by one as image and text with correct secret writing rule.

Step 3: Apply hash operate rule with correct key in cipher text to spot the key information.

Step 4: Identification of secret information.

In this method the hash fuction is apply to the most significant bits (MSB) term rather than LSB the information that ought to be hide in most significant bits (MSB).

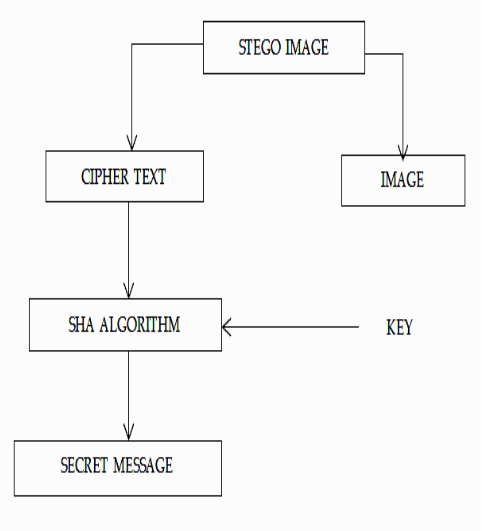

Fig.3. Decoding the Secret message

VI. SIMULATION RESULT

Simulation is performed by completely different color pictures. Figure.4. is that the original cowl image wherever its bar chart worth is live and shown in figure.5. the information is encoded with image and therefore the encoded image is shown in Figure.7. and its bar chart is figure.8. currently compare the figure four and half-dozen wherever kind of like one another and bar chart are similar. Its mean that our projected rule is effectively utilized in cryptography when secret writing the text the PSNR are measured wherever compare with previous methodology our rule offer high accuracy worth.

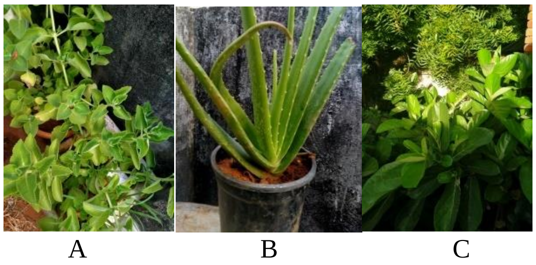

Fig.4. Original image

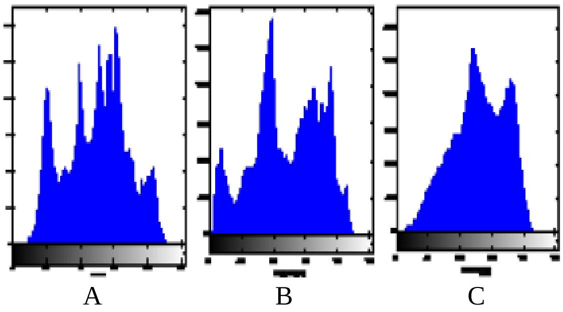

Fig.5. Histogram of original image

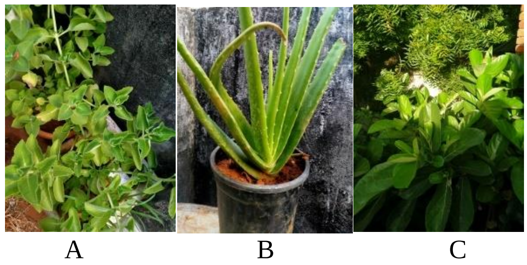

Fig.6. Encoded image with data

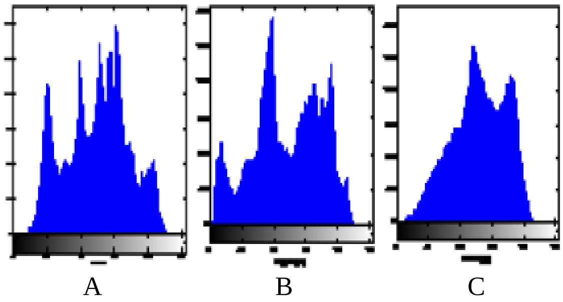

Fig.7. Histogram of encoded image with data

Table.1.PSNR value of the image

IMAGE NAME	HASH	MODIFIED HASH
A	47.5596	48.2645
B	41.5672	42.2756
C	38.5656	39.7012

VII. CONCLUSION

In the previous methodology the information is method with LSB term thus hacker will simply hack the information and procure the key text. however our methodology the information is hide in most significant bits (MSB) term and cypher with the changed hash operate wherever it will perform a lot of collision to cover the information. thus hacker will feel issue to cover and our rule offer smart security to information within the image and obtained a high accuracy result with simple implementation method.

VIII. REFERENCES

[1] Data Hiding and Retrieval, A.Nath , S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[2] Zhang Yun-peng, Liu Wei, Cao Shui-ping, ZhaiZheng-jun, NieXuan, Dai Wei-di, “Digital image encryption algorithm based on chaos and improved DES”, IEEE International Conference on Systems, Man and Cybernetics, 2009.

[3] N.V Rao, J.TL Philjon, “Metamorphic Crypto- A Paradox between Cryptography and Steganography using Dynamic Encryption”, IEEE Xplore International Conference on Recent Trends in Information Technology, June 2011, pp. 217-222.

[4] Alain,C.Brainos, “A study of Steganography and Art Of Hiding Information,” East Carolina University.

[5] NedeljkoCvejic and TapioSeppaanen, “Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding”.

[6] Pund-Dange, S. Desai, C.G. “Secured data communication system using RSA with mersenne primes and Steganography”. Computing for Sustainable Global Development (INDIA Com), 2015 IEEE 2nd International Conference on 11-13 March 2015.

[7] Yu-chi chen, chih-weishiu, gwoboahorng. “Encrypted signal-based reversible data hiding with public key cryptosystem” IEEE article Journal of visual communication and image representation, volume 25, issue 5, July 2014, pages 1164-1170.

[8] KritikaSingla, SumeetKaur, “A Hash Based Approach for secure image stegnograpgy using canny edge detection method,” International journal of computer science and communication , vol.3, no.1,pp.156-157,June 2012.

[9] Gabriel MachariaKamau, Stephen Kimani, WaweruMwangi, 2012, “An Enhanced Least Significant Bit Steganographic Method for Information Hiding”, www.iiste.org, ISSN 2224,5782, Vol 2, No.9.

[10] K.Dhanasekaran, P.Anandhan, A.Manju, “A Computational approach of Highly Secure Hash Algorithm for Color image steganography using edge detection and Honey Encryption Algorithm”, International Journal of Engineering and technology, 7(2.24)(2018) PP239-242.

[11] MrithaRamalingam, Nor Ashidi Mat Isa, “Video steganography based on integer Har wavelet transforms for secured data transfer”, Indian Journal of Science and Technology, Vol 7(7), 897904, July 2014.

[12] A. kasgar, J. Agrawal and S. Sahu “New Modified 256-bit MD5 Algorithm with SHA Compression
Function”, International Journal of Computer Applications (0975 – 8887) ,Vol.42,No.12, March 2012

[13] S. M. Bellovin and E. K. Rescorla.Deploying a new hash algorithm. Technical Report CUCS-036-05, Dept. of Computer Science, Columbia University, October 2005.

[14] E. Biham, R. Chen, A. Joux, P. Carribault, C. Lemuet, and W. Jalby. Collisions of SHA-0 and Reduced SHA-1. In *Proceedings of Eurocrypt '05*, 2005

[15] Data Hiding and Retrieval, A.Nath ,S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.