EFFICIENT AUTHENTICATION PROTOCOL USING CRYPTOGRAPHIC HASH FUNCTION & LSB DYNAMIC HOP IMAGE STEGANOGRAPHIC TECHNIQUE FOR SECURE COMMUNICATION

B. Madhuravani*, Dr. D.S.R. Murthy [†]

* *Department of CSE, MLR Institute of Technology,Dundigal, Hyderabad, Telnagana, India,madhuravani.peddi@gmail.com*
[†] *Department of CSE, Geethanjali College of Engineering & Technology, Keesara, Hyderabad, Telangana, India,dsrmurthy.1406@gmail.com*

Keywords: Steganography, Cryptographic hash function, Hop variable, LSB, Diffie–Hellman.

Abstract

A novel new verification convention utilizing a cryptographic hash function and a Steganography using a hop variable is displayed in this paper. This convention chooses a cryptographic hash work progressively and creates message digest. As opposed to LSB Steganography, we utilize a hop variable LSB steganography to implant private information into a stego object. This convention sets up a safe correspondence channel between two gatherings and trades information safely over the web.

1 Introduction

As the web clients are expanding every day we need a safe channel to store and trade the private data. Conventional and most basic way to deal with information is scrambling the information to make it insignificant, called as encryption. The mixed information can be comprehended by a man who knows how to get the first information from it, known as unscrambling. The significant downside with this methodology is despite the fact that he mixed information which is indistinguishable yet it is accessible to the outsiders [1]. The second approach is concealing the mystery data in an article over the transmission. The stego article is fundamentally the same as unique picture, consequently it is extremely hard to distinguish the mystery transmission [16]. Be that as it may, it is exceptionally hard to recoup message from an item when it is helpless against assaults, for example, revolution, interpretation, editing etc.,[2] Authentication is the underlying procedure to approve a client give security administrations in remote correspondence. There is a need of solid verification, to shield versatile correspondence from gate crasher exercises like information change, movement investigation or foreswearing of administration. With rising administrations, security prerequisites would be solid taking into account the applications. The principle motivation of cryptographic hash capacities is data reliability. These can be used as a piece of both secure and temperamental channel.These can be utilized as a part of both secure and shaky channel [3].A hash function is a function which maps a subjective length contribution to a length of altered yield. This hash function gives back a message review which can be dealt with as signature of the information [3]. Uses of cryptographic hash capacities incorporate Digital mark, message uprightness, confirmation conventions, watchword insurance and some more. Numerous confirmation conventions, for example, Kerberos utilizes hash functions. Thusly, different applications can be affected by shortcoming of hash capacity. Generally utilized hash capacities are MD−5, Secure Hash Algorithm−1 (SHA−1), SHA−2 hashing calculations. There is a requirement for a novel and more secure hash function to ensure against cryptanalytic assaults, particularly assaults of Wang et al. [4, 5, 6, 7]. National Institute of Standards and Technology (NIST) declared challenge, for another cryptographic hash capacity which is more secure and productive among the current. It reported keccak a triumphant calculation as the more secure standard hashing calculation SHA−3[16].With cautious configuration of hash capacity additionally, they are helpless against crash assaults. To give secure correspondence between two gatherings we propose an authentication protocol using cryptographic hash functions and hop based steganography. This strategy propose a productive system which secure our private information over the remote correspondence furthermore guarantees the genuineness.

Rest of the paper is sorted out as takes after. The introduction to cryptographic hash functions and steganography is discussed in Section 3 and 4. The proposed procedure has been discussed in Section 4. Section 5 introduces the test results, and execution of the proposed framework against other existing procedures. Conclusions are given in section 6 [17].

2 Cryptographic Hash Function: SHA-1

A hash function maps a variable-length contribution to an altered length yield. The hash function yields a unique mark of the information which maps the variable length contribution to a settled length yield [17]. Cryptographic hash functions assume a fundamental part in, message honesty, client confirmation, advanced marks, secret word security and producing pseudo arbitrary numbers. Hash function gives secure correspondence conventions, for example, Internet Protocol Security (IPSec), Secure Socket Layer (SSL). The handshaking convention in SSL utilizes a hash function to make a message verification code. To guarantee the trustworthiness of email messages in Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) hash functions are utilized broadly.
Scientifically a hash cfunction is characterized as MD = HF(M), where HF is a hash function hold the accompanying properties [8].

a. It is conceivable to figure MD from M yet it is difficult to compute M from MD.

b. Hard to discover messages M1 and M2 which creates same message digest i.e HF(M1)≠ HF(M2)

The best known calculations to create message digest are MD-2, MD-4, MD-5, SHA-0, SHA-1, SHA-2 and SHA-3. SHA-1 is the most broadly utilized hash calculation for respectability which produces a 160 piece message digest with 80 rounds and effective as far as time and vigorous [17].

3 Steganography: Generating Hop Variable

Steganography is a craft of concealing a private data in another medium like picture, sound, video. The word steganography is gotten from the greek words "stegos" signifying "spread" and "grafia" signifying "writing"[9] that is steganography is a "secured composing". The steganography comprises of three fundamental parts as appeared in Fig. 1[17].

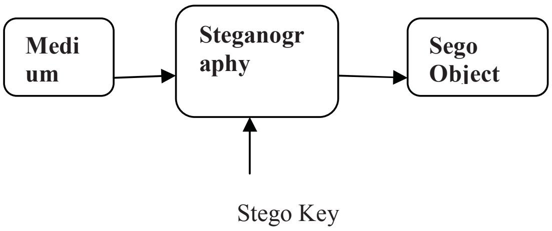

Fig 1: Steganography Model

3.1 Image Steganography Methods:

Steganography is a strategy which conceals the mystery data in a spread object of picture with organizations, for example, JPEG, PNG, GIF and so on., [Fig 2] this technique takes mystery message and cover object as the info and produces the stego object with the assistance of stego key which is given as contribution to removing calculation and concentrates the implanting mystery data by applying the same stego key [17].

a) Least Significant Bit Method: A well-known and straightforward strategy where the mystery data is installed into a picture document in LSB, however the burden with this technique is, it is touchy for any controls of picture like pressure, trimming and so on... [17]

b) Transformation Domain Technique: conceals mystery information in zones of the picture that are less presented to pressure, editing, and picture handling which complex contrasting and LSB technique [10].

3.2 Algorithm: Generate Hop Variable

Step 1: Read a value N

Step 2: Create SecureRandom object random

Step 3: Obtain Prime number P by invoking

BigInteger.probablePrime(N/2,random)

Step 4: Calculate P/2 and obtain Hop

Step 5: Exchange Hop securely by invoking Diffie-Hellman Key exchange.

4 Proposed Technique

This segment talks about our new confirmation convention for secure transmission of private data in remote correspondence. The proposed convention is delineated in Fig.2 and Fig.3.

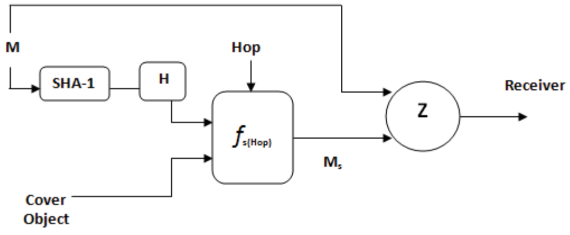

Fig. 2: Encoding Algorithm

Where

M = Original message

SHA-1 = Cryptographic hash function which generates hash code

Cover Object = Medium

fs(hop) = Hop based Steganography encoding algorithm

Ms = Stego object

Z = Concatenating both M and Ms and send to Receiver

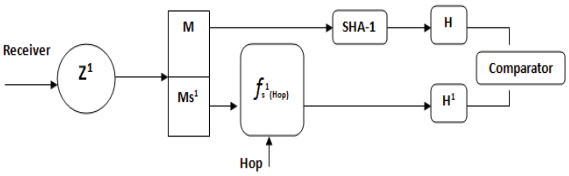

Fig. 3. Decoding Algorithm

4.1 Algorithm: Encoding

This strategy is delineated in fig 2 and functions as takes after [17]:

Step 1: During step 1 the mystery data (M) is hashed by selecting SHA-1 hash function and generates Message Digest H.

Step 2: The secret information (M) and Message Digest (H) is implanted into an image using dynamic hop image steganography technique and generates Ms

Step 3: Ms and M together are send to the receiver.

4.2 Algorithm: Decoding

This strategy is delineated in fig 3 and functions as follows:

Step 1: At reception of Ms is given inverse hop steganography model and retrieves H1.

Step 2: Calculate message digest for the received information H

Step 3: Comparator function compares the calculated and received message digest.

5 Simulation and Results

To examine the viability of proposed verification convention, we have led various trials. This segment exhibits the arrangement of investigations completed and the outcomes watched. Further, we examine the execution of our calculation and com-pared the outcomes with couple of unmistakable existing techniques.

The proposed strategy is reproduced in java with plaintext and image records. This has been tried for various images [17]. The original image is shown in Fig 4(a), 5(a) and their stego objects with different hash functions are shown in 4(b), 5(b).

Fig4a.Original Image (Tiger)

Fig4b.Stego Image (Tiger)

Fig5a.Original Image (Hibiscus)

Fig5b.Stego Image (Hibiscus)

5.1 Stego Object Generation

The time to generate stego object for a cryptographic function is depicted in the Table 1[16].

Table 1. Time to generate stego object

Size of Cover object	Text	Hop Variable	Time to generate stego object (ns)		Size of stego object
			LSB Steganography	Hop based Steganography	
Tiger 1.72 MB	Welcome	3	503256129	507127325	1.71 MB
Hibiscus 1.45 MB	Hello World	10	505257429	509127649	1.45 MB

6 Conclusions

In this paper, a proficient verification convention to open up collision resistance utilizing Cryptographic Hash Function and LSB Hop based Image Steganographic Technique is proposed. We propose an effective technique for the protected transmission of information between two gatherings. The proposed framework can be utilized to abstain from altering information or phishing assaults [16]. The proposed framework is actualized and tried for various cryptographic hash functions and hop based image steganography procedure.

References

[1] Mihir Bellare and Phillip Rogaway. Introduction to modern cryptography. Chapter 5: http://www-cse.ucsd.edu/users/mihir/cse207/w-hash.pdf, September 2005.

[2] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, Feb1998, pp. 26-34.

[3] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, volume 1109 of Lecture Notes in Computer Science, pages 1 – 15, Santa Barbara, California, USA, August 1996. SpringerVerlag.

[4] Xiaoyun Wang and Hongbo Yu, How to Break MD5 and Other Hash Functions, EUROCRYPT, pp. 19–35, 2005.

[5] Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, and Xiuyuan Yu, Cryptanalysis of the Hash Functions MD4 and RIPEMD, EUROCRYPT, pp. 1–18, 2005.

[6] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, Finding Collisions in the Full SHA–1, CRYPTO, pp. 17–36, 2005.

[7] Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin, Efficient Collision search Attacks on SHA–0, CRYPTO, pp. 1–16, 2005

[8] Krystian Matusiewicz, Analysis of Modern Dedicated Cryptographic Hash Functions, PhD thesis. Macquarie University, 2007

[9] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science,www.liacs.nl/home/ tmoerl/privtech.pdf

[10] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science,www.liacs.nl/home/ tmoerl/privtech.pdf

[11] Huynh-Thu, Q.; Ghanbari, M. (2008). "Scope of validity of PSNR in image/video quality assessment". Electronics Letters 44 (13): 800–801. doi:10.1049/el:20080522

[12] B. Girod, "What's wrong with mean-squared error?" in Visual Factors of Electronic Image Communications. Cambridge, MA: MIT Press, 1993

[13] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, Apr. 2004

[14] Hans Dobbertin. RIPEMD with two-round compress function is not collision-free. Journal of Cryptology, 10(1):51–70, 1997

[15] X. Wang, Y. Yin, H. Yu, Finding Collisions in the Full SHA-1. In Advances in Cryptology - CRYPTO '05, 2005

[16] B. Madhuravani, Dr. P. Bhaskara Reddy, "An Efficient Authentication Protocol to amplify collision resistance using Dynamic Cryptographic Hash Function & LSB Hop based Image Stegano-graphic Technique", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 7 (2016) pp 5293-5296. Research India Publications. http://www.ripublication.com.

[17] B. Madhuravani, D. S. R. Murthy, P. Bhaskara Reddy, "novel authentication protocol using multi cryptographic hashfunctions and

Steganography", International Journal of Advanced Computing (IJAC), Vol. 48, May 2015.