International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST218486

Confidentiality of Data using Hash Function

K. Ramprakaash[1], S. Ramkumar[1], R. K. Santhosh[1], P. Shanmuga Priya[2],
UG Scholar[1], Assistant Professor[2],
Rajalakshmi Engineering College, Chennai, Tamil Nadu, India

Article Info
Volume 8, Issue 4
Page Number : 606-610

Publication Issue
July-August-2021

Article History
Accepted : 16 Aug 2021
Published : 21 Aug 2021

ABSTRACT

Steganography and Cryptography are two major fields which is widely used for data security. With the help of these technologies, data security is provided in banking system. In the proposed method, the online transactions are done virtually using hash function. Encryption of data is done by using the cryptographic hash function algorithm. The proposed approach implements an efficient algorithm for embedding the data in an image using steganography which provides the better security pattern for sending messages through a network. The authentication details of the sender and the receiver is hidden to achieve a secure transmission. The proposed approach provides better integrity and confidentiality. This paper implemented a novel methodology which can be used as a secure and highly efficient method of data hiding and data extracting.

Keywords : Hash Function, steganography, security integrity.

I. INTRODUCTION

Nowadays there are many ways to transact money in a virtual manner like debit/credit card, net banking, BHIM UPI, etc. These methods are secure up to an extent, but when it comes to very large amounts, there arises a risk of security. But there is no efficient method for the transaction of money through cheque virtually. Combining the concepts of cryptography and steganography have come up with a secure method to transact large amounts of money through cheque virtually. Steganography is a technique in which a secret data is get hided into an image or any other media file. Whereas cryptography is a method of converting an existing plain text message into an encrypted unreadable form.

As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover-image and the image obtained after steganography is called the stego-image.In modern digital steganography, data is first encrypted or obfuscated in some other way and then inserted, using a special algorithm, into data that is part of a particular file format such as a JPEG image, audio or video file. The secret message can be embedded into ordinary data files in many different ways. One technique is to hide data in bits that represent the same colour pixels repeated in a row in an image file. By applying the encrypted data to this redundant data in some inconspicuous way, the result will be an image file

that appears identical to the original image but that has "noise" patterns of regular, unencrypted data.
The practice of adding a watermark a trademark or other identifying data hidden in multimedia or other content files is one common use of steganography.
Watermarking is a technique often used by online publishers to identify the source of media files that have been found being shared without permission. While there are many different uses of steganography, including embedding sensitive information into file types, one of the most common techniques is to embed a text file into an image file. When this is done, anyone viewing the image file should not be able to see a difference between the original image file and the encrypted file, this is accomplished by storing the message with less significant bites in the data file. This process can be completed manually or with the use of a steganography tool. In LSB method, least significant bits of information in the carrier image is substituted by secret message.

II. LITERATURE REVIEW

In the paper titled 'Comparative Study of Various Steganography Techniques', Ekta Dagar, Sunny Dagar, various types of steganography techniques are explained. Those techniques are LSB substitution, Masking and filtering, Algorithm transformation methods. LSB method is briefly explained in this paper. LSB is the most popular technique used to hide the secret information into an image by replacing the least bits of the image with the secret information bits. Since when the least bit is changed it does not create a drastic change in the intensity value of the image.

In the paper titled 'A Study on Steganography Concealing Data', Anu Sara Alexander and L.C. Manikandan,2019, the various techniques to embed different type of digital files like audio, video, text, image was explained. It mainly explains about the spatial domain methods instead of frequency domain methods. In audio steganography, the audio file is converted into bit pattern and each character in the message is embed into the bit pattern. In video steganography a secret message is being concealed inside a digital video to produce stego video using data embedding technique.

In the paper titled 'Cryptographic hash functions: A Review', Rajeev Sobti and G Geetha, detailed study on various cryptographic hash functions is explained. Cryptographic hash functions are of three types, namely One-way hash functions, Collision resistant hash functions and Universal One-way hash functions. The various security services of hash functions like Achieving integrity, Authentication and Implementation of Digital signatures are explained. With the Security services available the prevention various methods of attacks on hash functions like Brute force attack and Cryptanalytical attack are briefly explained in this paper.

III. PROPOSED SYSTEM

It is based on steganography and hashing techniques to provide data confidentiality and data integrity. To achieve this the secret data is encrypted and embedded in an image. For this we need an image of the cheque, the unique ID of the sender and his digital signature, the unique ID of the receiver and his name exactly as given to the bank's database. First the hash value is generated for the sender's unique ID and his digital signature using a hashing algorithm. Here, the hashing process is executed by using the algorithm 'Message Digest 5' also known as MD5. The MD5 algorithm can have 128 bits length of the message digest. The reason why we are considering MD5 in our case is because of the following two major reasons. Firstly, comparing to the other existing hashing algorithms it is much simpler. The second and the main advantage of selecting MD5 is that it is much faster compared to SHA or any other hashing algorithm. The hash value that is generated from the

MD5 algorithm is a 16-bit Hexa decimal value.The hash value of the sender's unique ID is concatenated with hash value of the image. Now the hash value for the sender side is generated, similarly the hash value is generated for the receiver's unique ID and his account name. Now we have generated two hash values, one for the sender side and the other for the recipient.

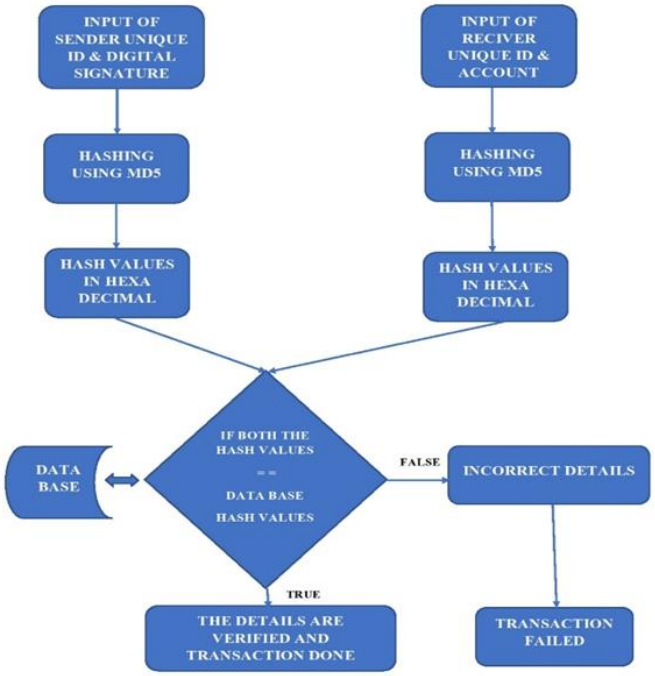

Figure 1. Schematic Diagram

After the hash values are embedded into the image of the cheque, the image is transmitted over to the bank. On receiving the image, the bank decrypts the image to extract the hash values. The bank will be having a set of hash values in their data base. Now the bank compares the hash values extracted from the image with the hash values on their data base. If both the hash values match with that of the bank's data base, then the details are verified and the transaction is done. If the values mismatch, then the transaction is declined. Thus, the transaction is done securely. For the secure transmission of the data, the hash values must be embedded inside the image of the cheque. To do so, in our case we will be following the 'Least Significant Bit' method which is also known as the LSB method. LSB works on the time domain. The reason for selecting LSB in our case is that in LSB only the least significant bit or the last bit value of the pixel is replaced. The pixel values are replaced by bits of the two hash values that were generated. As we have replaced only the last bit value of the pixel, there will not be much of a change in the image that will be visible to the human eye.

IV. RESULT AND DISCUSSION

The image of the cheque with the hash values of the authentication details of the sender and the receiver is received on the bank side . The bank decrypts the image and cross checks the hash values with their data base.

5.HISTOGRAM ANALYSIS

The statistical features of the stego and the cover images can be analyzed and compared by drawing their histograms. To ensure the resistivity of the steganographic technique against the statistical attack, the histogram of stego and its corresponding cover image should not have any significant change. It can be noted that, there is no change of values in terms of pixels and size between the stego and cover images. Accordingly, it is very difficult for the attackers to detect the difference between the original images and the stego images. This means that, the proposed algorithm improves the protection of secret data and establishes a secure communication channel

HISTOGRAM OF NORMAL IMAGE

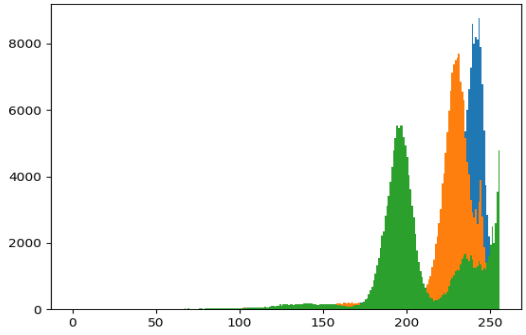

Figure 2. Histogram of Normal Image

HISTOGRAM OF STEGO IMAGE

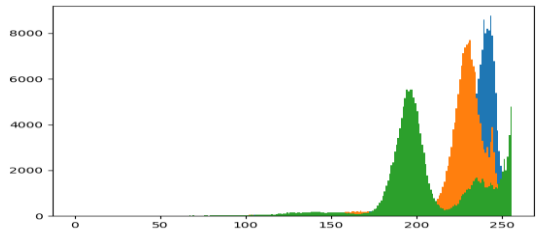

Figure 3. Histogram of Stego Image

V. CONCLUSION

Thus, the proposed method implemented a model to execute the transaction of money through Cheque virtually in a secure way by combining the methods of cryptography and steganography. The computational model implemented in this project chosen after extensive research, and the successful testing results confirm that the choices made by the researcher are reliable. In the future the model can be made even secure based upon implementing any new algorithms or data hiding method which may be brought into existence in the near future. The proposed model gives us an insight into what the future may hold in the digital banking domain. With a few more extensions the model can be used in real time banking environments.

VI. REFERENCES

[1]. Gupta, S. and R. Jain, 2015, 'An innovative method of Text Steganography', Proceedings of the 2015 3rd International Conference on Image Information Processing , December 21-24, 2015, IEEE, Waknaghat, India, pp: 60-64.

[2]. Koley, S. and K.K. Mandal, 2016. 'A novel approach of secret message passing through text steganography', Proceedings of the International Conference on Signal Processing, Communication, Power and EmbeddedSystem (SCOPES), October 3-5, 2016, IEEE, Paralakhemundi, India.

[3]. Mandal, K.K., A. Jana and V. Agarwal, 2014. 'Text Steganography based on mathematical model of number system', Proceedings of the 2014 International Conference on Circuits, Power and Computing Technologies (ICCPCT'14), March 20-21, 2014, IEEE, Nagercoil, India.

[4]. Por, L.Y. and B. Delina, 2008. 'Information hiding in text steganography', Proceeding of the7th WSEAS International Conference on Mathematics and Computers in Science and Engineering, April 6-8,2008, World Scientific and Engineering Academy and Society, Hangzhou, China.

[5]. Sharma, S., A. Gupta, M.C. Trivedi and V.K. Yadav, 2016. 'Analysis of different text steganography techniques', A survey. Proceedings of the 2016 2nd International Conference on Computational Intelligence and Communication Technology (CICT), February 12-13, 2016, IEEE, Ghaziabad, India.

[6]. Singh, H., A. Diwakar and S. Upadhyaya, 2014. A novel approach to text steganography. Proceedings of the 2014 1st International Congress on Computer, Electronics, Electrical and Communication Engineering, March 17-18, 2014, Chennai, India.

[7]. C. Qin, P. Ji, C. C. Chang, J. Dong, and X. M. Sun, 'Non-uniform Watermark Optimal Iterative BTC for Image Tampering Recovery',IEEE Multimedia, 2018.

[8]. Xintao Duan, Kai Jia, Baoxia Li1, Daidou Guo,En Zhang,and Chuan Qin 'Reversible steganography Scheme Based on a U-Net Structure ', IEEE Access, 2017.

[9]. E. P. Singh and E. P. S. Saini, 'A Novel Approach to Robust and Secure Image Steganography Based on Hash and Encryption',Int. J. Eng. Sci. Res. Technol., vol. 5, no. 3, pp. 194–201, 2016.

[10].J. Al-Saraireh, 'An efficient approach for query processing over encrypted database', J. Comput. Sci., vol. 13, no. 10, pp. 548–557, 2017.

[11].R. Indrayani, H. A. Nugroho, R. Hidayat, and I. Pratama, 'Increasing the security of MP3 steganography using AES Encryption and MD5 hash function', in Proceedings - 2016 2nd International Conference on Science and Technology-Computer, ICST 2016, 2017, pp. 129–132.

[12].S. S. Saraireh, and M. S. Saraireh, 'Filter Bank Block Cipher and LSB Based Steganography for Secure Data Exchange', Int. J. Commun. Antenna Propag., vol. 7, no. 1, p. 1, Feb. 2017.

[13].C. Qin, C. C. Chang, and Y. P. Chiu 'A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting', IEEE Transactions on Image Processing, vol.23, 2014.

Cite this article as :

K. Ramprakaash, S. Ramkumar, R. K. Santhosh, P. Shanmuga Priya, "Confidentiality of Data using Hash Function", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 4, pp. 606-610, July-August 2021. Available at doi : https://doi.org/10.32628/IJSRST218486
Journal URL : https://ijsrst.com/IJSRST218486