Volume 6, Issue 2, February 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Hiding System Based on Double MD5 Hashes and LFSR Generators

Ismael Abdul Sattar[*], **Jamal Nasir Hasoon**

Department of Computer Science, College of Science, University of Al-Mustansiriyah,
Baghdad, Iraq

Abstract— This paper show the multi-level hashes using MD5 that play the role to increase the complexity for the security system, by forming the first map and LFSR will build the second map, which used to guide hiding process. First hashes output from MD5 will not only feed linear feedback shift registers (LFSR) which form the second map that determine the target hiding pixels but also indexing set of other pixels within cover image that will get hashes for each one of them to form a first map that will determine the target bit within the pixel. Proposed System shows a good value rang for MSE as well as PSNR as objective metric measurements.

Keywords— Steganography, MD5, hash function, LFSR.

I. INTRODUCTION

Information hiding represents a class of processes used to embed data into various forms of digital data such as image, audio, and video. In digital images the information hiding applications could be divided into two groups depending on the relationship between the embedded message and the cover image [1]. The first group is formed by steganography application in which the message has no relationship to the cover image and the cover image plays the role of a decoy to mask the very presence of communication [4]. The content of the cover image has no value to the sender or the decoder.

In this typical example of a steganographic application for covert communication, the receiver has no interest in the original cover image before the message was embedded. Thus, there is no need for lossless data embedding techniques for such applications. The word steganography comes from the Greek name "steganos" (hidden or secret) and "graphy" (writing or drawing) and literally means hidden writing. Steganography uses techniques to communicate information in a way that is hidden [2], [3]. The second group of applications is frequently addressed as digital watermarking. In a typical watermarking application, the message has a close relationship to the cover image. The message supplies additional information about the image, such as image caption, ancillary data about the image origin, author signature, image authentication code, etc. While the message increases the practical value of the image, the act of embedding inevitably introduces some amount of distortion [5].

Both steganography and watermarking describe techniques that are used to imperceptibility convey message by embedding it into the cover image. But steganographic methods are interested in extracting the message, so usually it’s not robust against modification of the image. Watermarking, as opposed to steganography, is used for authentication and has the additional requirement of robustness against possible attacks [6], [7].

Using digestive algorithm to produce hashes it is a good decision to use as a map in hiding mechanism because it is one-way function even though no need to send it but it is implied with in the stego object [8], [9]. As linear feed back shift register (LFSR) producing a good complex sequence of bits that could play a role in hiding process [9].

II. PROPOSED SYSTEM

The proposed system can explained with the algorithm below as well as the block diagram in figure (1). Such that system shows the hiding process done using map that constructed based on MD5 algorithm. The suggested system doesn't require any shared information between the sender and receiver because the image size will represent the starting point to construct not only first map but also the second map.

Algorithm

Input

Image cover (gray of size W. H)

Secret message (text)

Output

Stego-object

Process

1. Read image size W, H. such that W, H represents width and height of the cover respectively.
2. Feed W, H. into message digest algorithm MD5, to get 32 hexadecimal digits (128 binary bits)
3. The output of the step 2 will index 6 pixels within the cover image using 20 bits (10 for first Dimension, 10 for second Dimension) each and the last 8 bits out of 128 ignored.

4. Feed each pixel value output of step 3 into MD5 to get map1 with size (6*128=768 bit).
5. Feed hashes from step (2) of size 128 bits into 4 LFSR of size 32 each as seed key.
6. Join function for each LFSR will determine using first 40 bits out of 128 bits (5 bit for index one cell and for two cells in each LFSR need 10 bits thus total of four LFSR required 40 bits).
7. First and second LFSR's will be indexing first dimension as well as third and fourth LFSR's will be indexing second dimension of the cover image that will be map2, to detriment the target pixel which used in hiding process. Excluding the 6 pixels in step (3).
8. Use two bits of the map (output of the step 4) to indexing the target bit within a pixel (output in step 7). One pixel will hide one secrete bit.

End

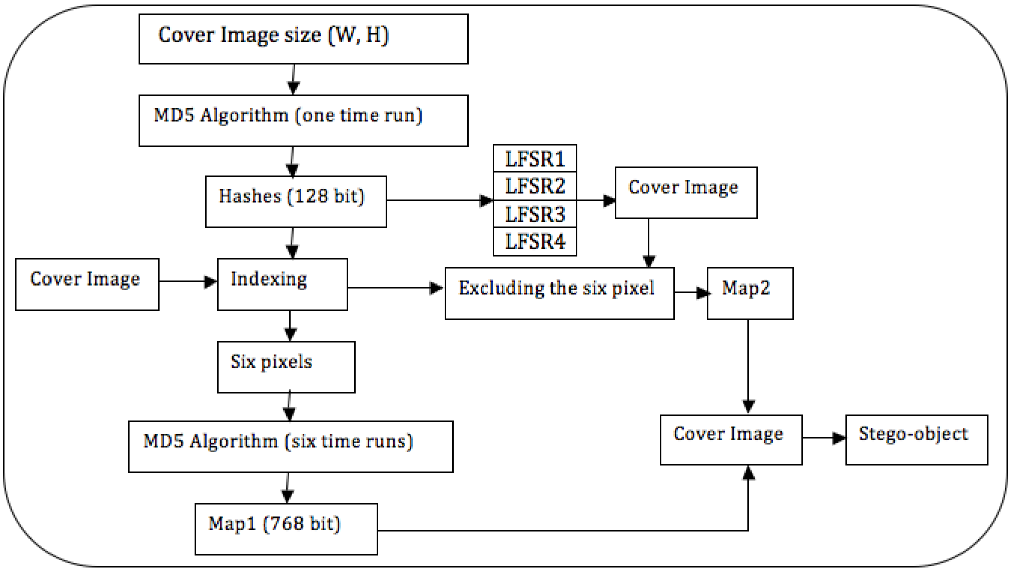

Figure 1. Show the block diagram for the proposed system

III. RESULTS

The proposed system feed with hundred gray images of different size (twenty of each size) the best five samples show in table (1) based on the PSNR value.

Image size In pixel	Hashes $(.Map - 1.)$	Secret message size In byte	PSNR
128*128	**ffe2ddd2f0fc994cec3e30e8c1f3b614**	**1421**	**51.241**
200*245	**21eea91a8eb62f9b0af9f76d3841dfc3**	**4610**	**58.614**
256*256	**8599bc0ca2c2ef768d0610ffb916e4ef**	**5100**	**61.226**
260*310	**1a75ad5182d0e4c0a72fbda140f92c71**	**6789**	**65.498**
512*512	**f6d2e28bf3cdf08685bf3041d92365d3**	**21816**	**69.821**

The first row represents the survived (best PSNR) image out of twenty images with size 128*128 and secret message size 1421 byte and so on for the rest rows of the table.

IV. CONCLUSION

In our proposed system it doesn't required sharing any information between sender and receiver and this good point for two main reasons; first, reduce the rise suspicious sensing over the transmitting channel. Second, there is no stating point that the attacker might use for extracting the code. The system secure enough depend on the user demands which level of security that may fill full his requirements. One level of encryption that may add to the suggested system to increase the complexity. Another point that across mind is the capacity of the secret message that we want to hide one pixel will hide only one bit. It is done intentionally to balance the objective quality measurements like MSE and PSNR.

REFERENCES

[1] Katzenbeisser S. and Petitcolas F., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, USA, 2000.

[2] Jonathan. C, Patrick .D, Samuel .L and Robert .P, “Steganography and Digital Watermarking ", University of Birmingham, School of Computer science, URL: http://www.gnu.org/copyleft/fdl.html, 2004.

[3] Stefano Cacciaguerra and Stefano Ferretti, "Data Hiding: Steganography and Cryptography Marking", Department of computer science, university of Bologna, 2000.

[4] Eric Cole, "Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley Publishing, Canada 2003.

[5] Alexia .B, Panagiotis. T and Athanasios .s, "Hiding Message in Heavy-Tails: DCT-Domain Watermarking Detection Using Alpha- Stable Models”, IEEE Transactions on Multimedia, June 2003.

[6] Mohanty Saraju P.,"Digital Watermarking A Tutorial Review", University of South Florida Tampa, FL 33620, 1999.

[7] Nameer N. EL-Emam "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" Applied Computer Science Department, Faculty of Information Technology Philadelphia University, Jordan, 2007.

[8] Shin, N, "One-time Hash steganography", Information Hiding, Third International Workshop, Lecture Notes in computer. Science vol. 2000.

[9] Muttoo S.K.and Abdulsattar ,Ismael,(2012), „A new stegosystem based on LFSR genrator‟,International Journal of Engineering and innovative Technology Vol. 1, No.1, January, 2012.