Transmission and Authentication of Text Messages through Image Steganography

Pragya Agarwal
Amity University, U.P.,India

Shilpi Gupta
Amity University, U.P.,India

Anu Mehra
Amity University, U.P.,India

ABSTRACT

The demand for effective information security schemes is increasing day by day, with the exponential growth and use of Internet. Cryptography and Steganography are two popular techniques, which are to be used for effective secret communications. . In this paper I have proposed a scheme, which can encode a text message and transmit it safely to its destination. Moreover the receiver can authenticate the received message to ensure that any intruder has not altered the original message. To facilitate the authentication facility, a hash code will be generated by the original message, which will be sent to the receiver securely. The hash code will be sent to receiver by hiding it into an image using image steganography. The receiver will decrypt the cipher text message to get the plaintext message. After that receiver will calculate the hash code with the received message and will compare this, with the received hash code. If both the hash codes are equal, it means that the received message is the original message. For generating the hash code, I have used SHA-1 method, and also analysed its performance and compared with that of MD5 method.

Keywords

Image Steganography, Authentication, Hash Functions, Information Security.

1. INTRODUCTION

With the increasing reliance on digital media and the continued use of Internet to share information over it, the security of data and message authentication has become the real challenge for today's researchers. Hash function is a technique used to check the authenticity the data. The two most popular families of protocols to generate the hash function are SHA and MD. With the help of hash function, the receiver can ensure that the received data is original and it has not been altered while being transported. The generated hash function can be sent to the receiver securely by hiding it into another media such as an image or video using steganography.

2. WHAT IS A HASH FUNCTION

A Hash function is a function which converts an input text into a fixed sized, unique output value, called the hash code. Even a small change in the input text message will give a totally different output hash code.

Hashing is a special form of Encryption. It is often used for passwords. Hash function is a one way method to produce a fixed length message digest from a variable sized input text messages.

3. INTRODUCTION TO SHA1 AND MD5 ALGORITHM

MD5 belongs to the MD family of hash functions. It is a simple, fast and most widely used hashing method which generates 128 bit hash or message digest. It is the successor of MD4 method of hashing of the same MD family. Some research proved that MD4 is not that much secure and can be easily attacked, so MD5 was invented in 1991. However, in 2004, MD5 was also found to be insecure, as it can produce same hash value for 2 different messages resulting in collision, because of the small length of the generated message digest (128 bits).

SHA1 belongs to the SHA family of Hash functions. It produces a 160 bit long hash value or message digest. It is a very much strong and secure hashing algorithm. It can generate hash for any text message(<264 bits). It is much more secure and collision resistant as compared to the MD5 hash algorithm. However SHA1 is slower than MD5 and is difficult to implement. SHA-1 now has even higher strength brothers, SHA-256, SHA-384, and SHA-512 for 256, 384 and 512-bit digests respectively.

4. THE PROPOSED METHOD

4.1 Hashing Algorithm(Sender side)

1. Read the text file.

2. Calculate the hash code for the text in the file using SHA-1 algorithm.

4.2 Embedding Algorithm (Sender Side)

1. Convert the generated hash code into binary form.

2. Take an input image.

3. Convert the image into binary matrix form.

4. for I=0 to the length of hash code

a .Insert each bit in the least significant bit position of each pixel.
b. If the bit value of the hash code and the pixel LSB

value are same, then no need to change.

c. Otherwise, If the bit value of the hash code and the pixel LSB value are different, then replace the pixel LSB value with the hash code bit value.

5. Save the resultant embedded image.

6. Send the image to the receiver.

4.3 Enciphering Algorithm (Sender Side)

1. Read the text file.

2. Compute the cipher text using any encryption algorithm (I've used DES encryption algorithm).

3. Send the computed cipher text to the receiver.

4.4 De embedding algorithm (Receiver Side)

1. At the receiver side, take the image sent from the sender side.

2. For each pixel of the received image, extract the least significant bit and store it in a string s.

3. Convert the binary value of the string s into hexadecimal form.

4. Return the final string.

4.5 De Ciphering Algorithm (Receiver Side)

1. At receiver side take the cipher text sent from the sender side.

2. Compute the corresponding plain text using the corresponding decryption algorithm.

3. Return the generated plain text.

4.6 Hash Verification of the received message

1. Compute the hash code from the received text using the SHA-1 hashing algorithm.

2. Compare this computed hash code with the hash code extracted from the image.

3. If both the hash codes are identical then the message received is the original message sent from the sender.

4. Otherwise, if the hash codes are not identical, then the message received is not the original message and has been altered by some unauthorised person.

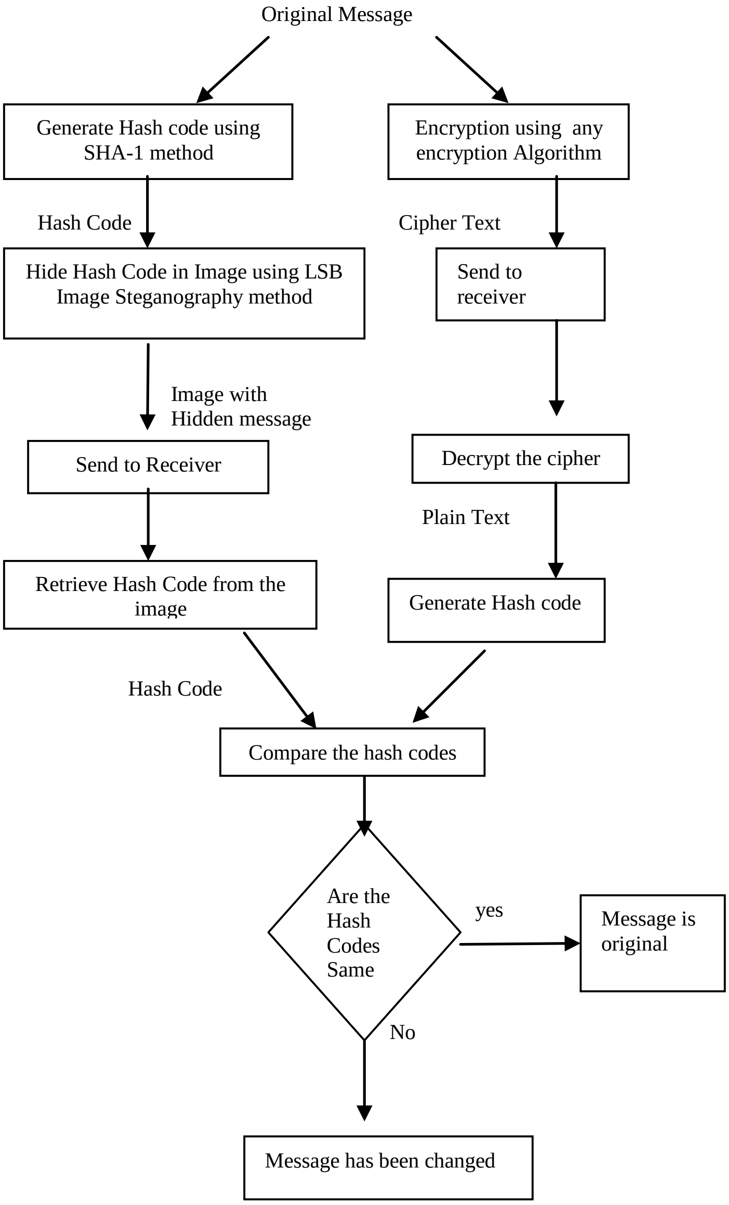


Figure 1: Flow Chart of the Method

5. ANALYSIS AND COMPARISON OF RESULTS

In this paper, message is converted into hash value using sha1 algorithm, and is sent to the receiver using image steganography. The proposed scheme has been implemented in java. There are following differences between SHA1 and MD5 hashing algorithm.

1. MD5 is simple and easy to implement while SHA1 is difficult to implement because of internal working of the two algorithms.

2. MD5 is faster than SHA1.

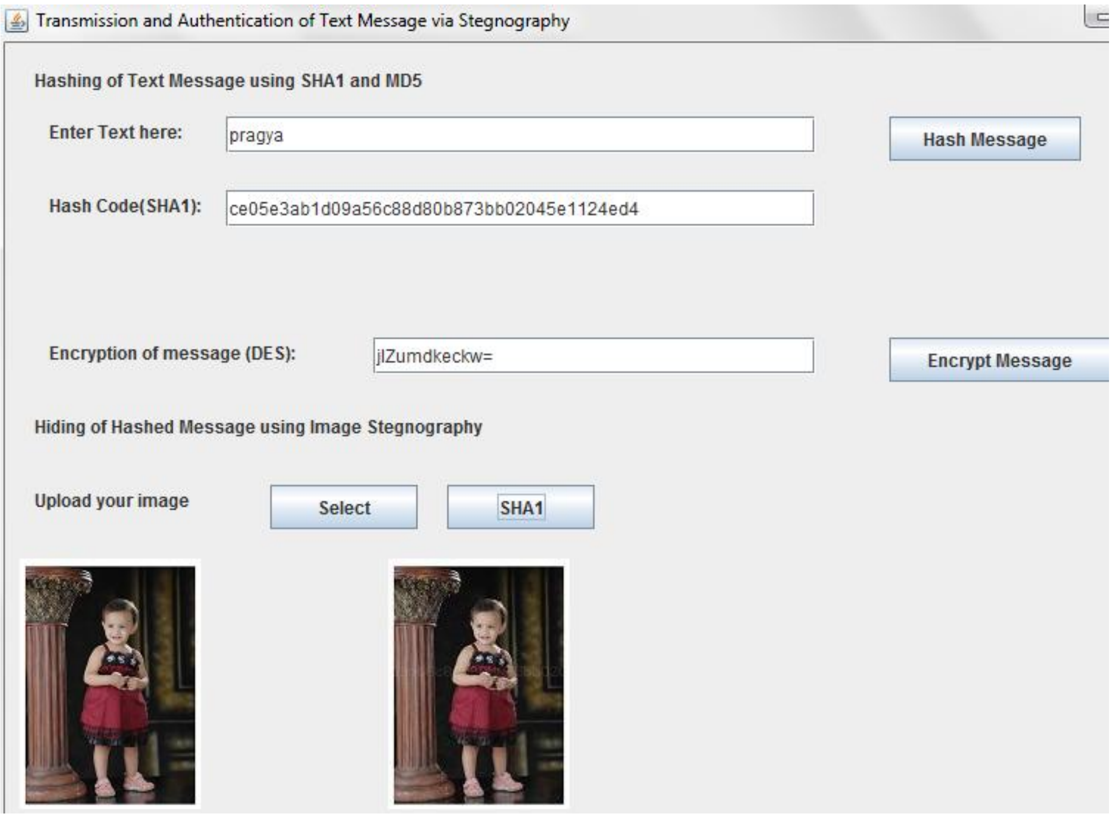
3. MD5 is more vulnerable to attacks than SHA1.

4. In SHA1 chances of collision are less as compared to MD5 because of larger sized message digest.

In MD5 output is 128 bits long while in SHA1 it is 160 bits so obviously the chances of collisions are less in SHA1 (1 in 2^{80} messages). MD4 and MD5 have already been proved as in secure in 2004,and are more likely to have collisions. The complexity of locating collisions are 2^{2} and 2^{30}. Since then SHA1 was the most popular and widely used algorithm for finding hash functions. But it was proved in [4] that message collisions are of the complexity 2^{69}. After that the collisions complexity has been proved to be 2^{63} in [5]. After SHA1, its successor SHA2 has also been invented which has even lesser chances of collisions. The security analysis of these algorithms can be done by using different techniques like pre-processing [3].

6. CONCLUSION AND FUTURE SCOPE

In this paper, both SHA1 and MD5 techniques are compared to generate hash values which is used to authenticate the text message. The pros and cons of both the techniques are also discussed. SHA1 algotithm is more secure than MD5, which in turn is faster than SHA1. The hash value or message digest is sent to the receiver through image steganography using LSB technique. The message can be encrypted by any technique and the generated cipher text can sent to the receiver and can also be authenticated using hashing techniques. It has been proved that no hashing technique of SHA and MD family or any other , is 100% Collison resistant. Researchers are doing a lot of work to find any such hashing algorithm. Already there has been a lot of improvement in its complexity of locating a collision, like SHA2 is still more secure than SHA1. Although it seems impossible to find an algorithm in which there are no chances of collisions. Still a lot of research is required so that a much more secure and fast technique can be found.



Transmission and Authentication of Text Message via Stegnography

Hashing of Text Message using SHA1 and MD5

Enter Text here: pragya

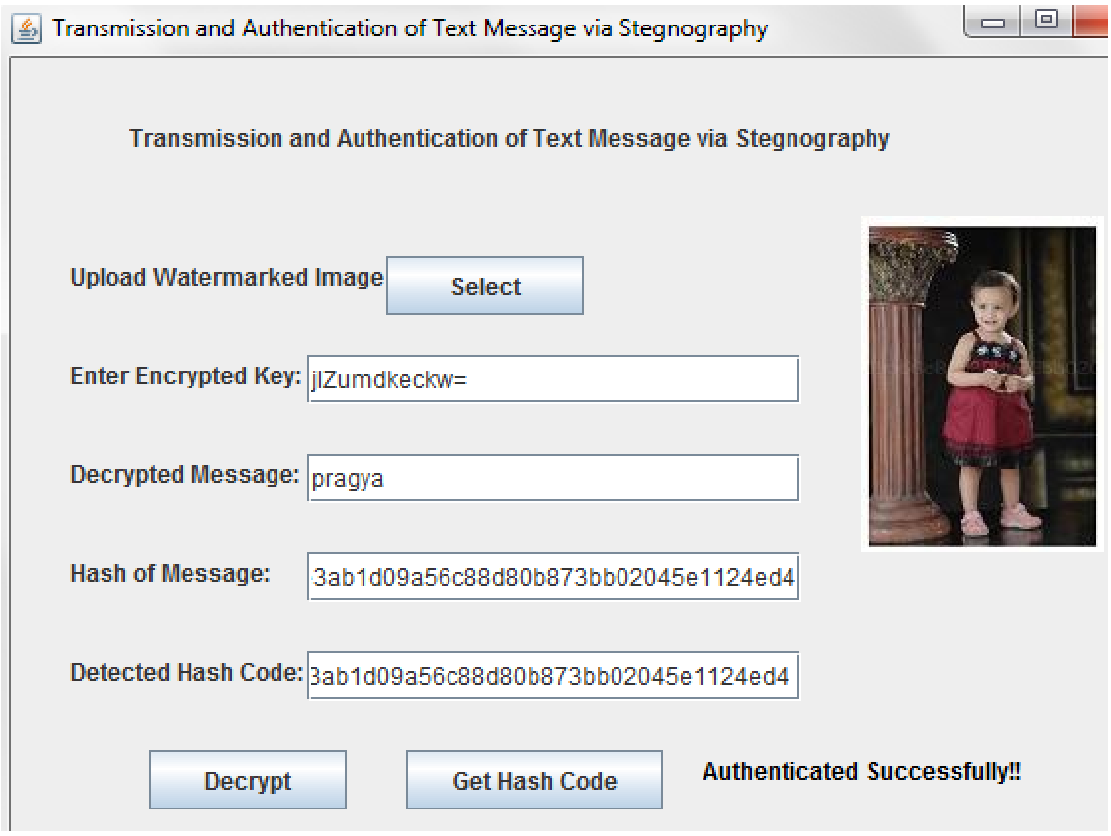
Hash Code(SHA1): ce05e3ab1d09a56c88d80b873bb02045e1124ed4

Encryption of message (DES): jlZumdkeckw=

Hiding of Hashed Message using Image Stegnography

Upload your image

Figure 2: Hiding of message and it's hash code in the image



Transmission and Authentication of Text Message via Stegnography

Transmission and Authentication of Text Message via Stegnography

Upload Watermarked Image

Enter Encrypted Key: jlZumdkeckw=

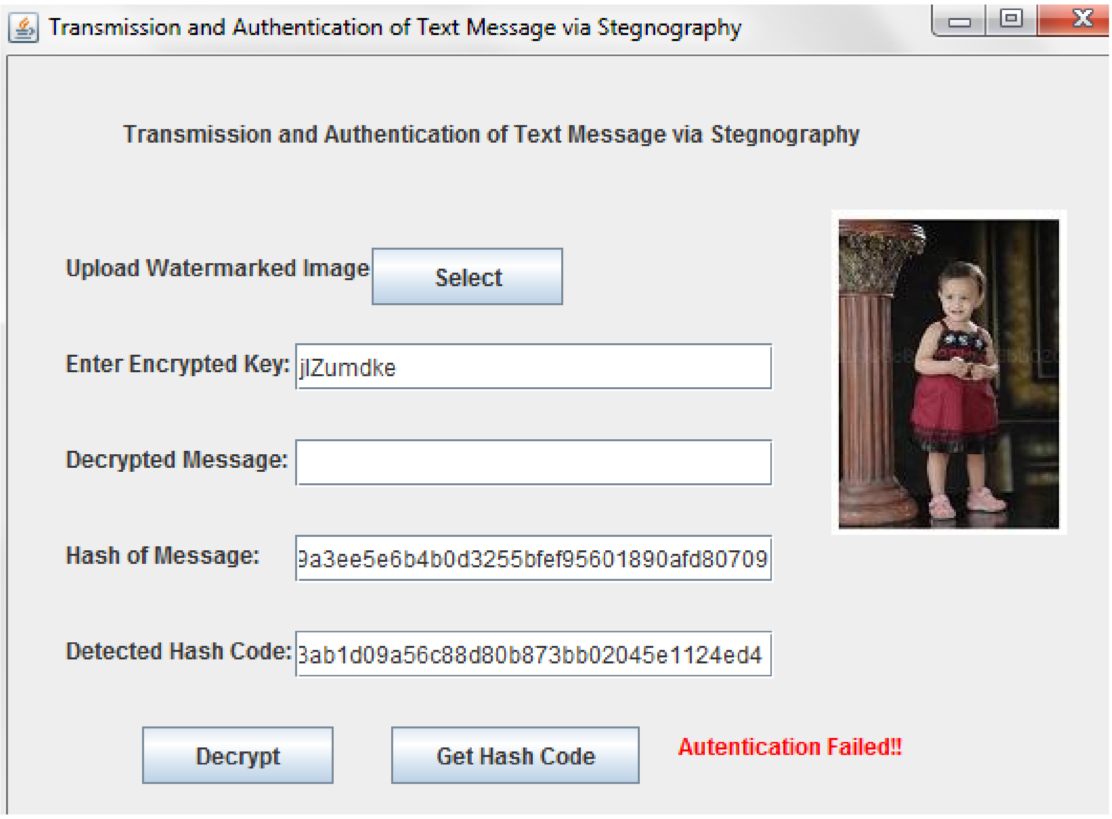
Decrypted Message: pragya

Hash of Message: 3ab1d09a56c88d80b873bb02045e1124ed4

Detected Hash Code: 3ab1d09a56c88d80b873bb02045e1124ed4

Authenticated Successfully!!

Figure 3: Retrieving hash code from the image and authenticating the message



Transmission and Authentication of Text Message via Stegnography

Transmission and Authentication of Text Message via Stegnography

Upload Watermarked Image

Enter Encrypted Key: jlZumdke

Decrypted Message:

Hash of Message: 9a3ee5e6b4b0d3255bfef95601890afd80709

Detected Hash Code: 3ab1d09a56c88d80b873bb02045e1124ed4

Autentication Failed!!

Figure 4: Checking authentication with wrong encrypted message

7. REFERENCES

[1] Sadaquat Ur Rehman, Mohammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman "Comparison based analysis of Different Cryptographic and Encryption Techniques using Message Authentication Code (MAC) in wireless sensor networks (WSN), International Journal of Computer Science issues 2012.

[2] Dinesh Dasarathan, "Analysis of Timing variability for Encryption Algorithms for the Atmega Platform", a project proposal for Real Time Operating System.

[3] Michael Sjydlo, Yiqun Lisa Yin, "Collision Resistant Usage of MD5 and SHA1 via message preprocessing", The Cryptographer's Track at RSA Conference - CT-RSA, pp. 99-114, 2006.

[4] X.Wang and Y.L. Yin, and H. Yu, "Finding collisions in full SHA1" in Advances of Cryptology-Crypto'05, Springer-Verlag, 2005.

[5] X. Wang, A Yao, F. Yao, "New collision search for SHA1", Rump Session Crypto'05.

[6] Kalavathi Alla, G. Gowri Shankar, G. Bala Subrahmanyam, "Secure Transmission of Authenticated Messages using new encoding scheme and steganography", CCSEIT-12, ACM , October 26-28, 2012, Coimbatore, Tamilnadu, India.

[7] A. Joseph Raphael, Dr. V. Sundaram," Cryptography and Steganography- A Survey", International journal of computational technology and Applications, vol. 2, p.p. 626-630, June, 2011.

[8] Soumik Das, Pradosh Bandyopadhyay, Prof. Atal Chaudhary, Dr. Monalisa Banerjee, "A Secure key based Digital Text Passing System through color Image Pixels", IEEE International conference on Advances in Engineering, Science and Management (ICAESM-2012), p.p.978-981, March 30,31, 2012.

[9] Fahim Irfan Alam, Fateha Khanam Bappee, Farid Uddin Ahmed Khondker, "An Investigation into Encrypted Message Hiding Through Images Using LSB", International Journal of Engineering Science and Technology (IJEST) vol 3, Feb 2011.

[10] Shamim Ahmed Laskar and Kattamanchi Hemachandran, " Secure Data Transmission using Steganography and Encryption Technique", International journal on Cryptography and Information Security (IJCIS), vol 2, September 2012.

[11] H.E. Michail, A.P. Kakarountas, A. Milidonis, C.E. Goutis, " Efficient Implementation of the keyed hash message authentication code (HMAC) using the SHA-1 Hash Function", IEEE, May, 2004.

[12] Hiroyuki Kobayashi, Hitoshi Kiya, " Robust Image Authentication using Hash Function", IEEE, Aug, 2004.

[13] M. Zeghid, B.Bouallegue, A. Baganne, M. Machhout, R. Tourki, " A Reconfigurable Implementation of the new Secure Hash Algorithm", Second International Conference on Availability, Reliability and Security (ARES 07), IEEE, Feb, 2007.

[14] J.K. Mandal, Madhumita Sen Gupta," Authentication/Secret Message Transformation through Wavelet Transform based Subband Image Coding (WTSIC)", Internatianal Symposium on Electronic System Design, IEEE, Feb, 2010.

[15] Debnath Bhattacharyya, Jhuma Dutta, Poulami das, S.K. Bandyopadhyay, Tai hoon Kim," Discrete Cosine Transformation based Authentication and secret Message Transmission Scheme", First International conference on Computational Intelligence, Communication Systems and Networks, IEEE, June, 2009.

[16] Cheng Xiao hui, Deng Jian zhi, "Design of SHA-1 Algorithm based on FPGA", Second International conference on Networks Security, Wireless Communications and Trusted Computing, IEEE, May, 2010.

[17] Sachin Tripathi, G.P. Biswas, Sumitra Kisan, " Cryptographic Keys Generation using Identity", Proc. Of Int. conference on Advances in Recent Technologies in communication and computing, IET, 2011.

[18] S.S. Manvi, M.S. Kakkasageri, D.G.Adiga, " Message Authentication in vehicular Ad hoc Networks: ECDSA based Approach", International conference on Future Computer Communication, IEEE, March, 2009.

[19] Hung Yu Chien, " Forgery Attacks on Digital Signature Schemes without using One way Hash and Message Redundancy", IEEE Communications Letters, vol. 10, May, 2006.

[20] Andhe Dharani, P.S. Satyanarayana, Andhe Pallavi, " Analysis of Message Authentication in Turbo Coded Halftoned Images using Exit Charts", World Academy of Science, Engineering and Technology, 2007.

[21] Ms. B.Veera Jyothi, Dr. S.M.Verma, Dr. C. Uma Shanker,"Implementation and Analysis of Email Messages Encryption and Image Steganography Schemes for Image Authentication and Verification", International Journal of Computer Applications, vol. 5, August, 2010.

[22] Babloo Saha, Shuchi Sharma," Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, vol 62, p.p. 11-18, January 2012.Defence Science Journal, vol 62, p.p. 11-18, January 2012.

[23] Rosziati Ibrahim, Teoh Suk Kuan, " Steganography Algorithm to Hide Secret Message inside an image", Computer Technology and Application, p.p. 102-108, 2011.

[24] T. Morkel, J.H.P. Eloff, M.S. Olivier, " An Overview of Image Steganography", Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA), July 2005.

[25] Nagham Hamid, Abid Yahya, R.Badlishah Ahmad, Osamah M. Al-Qershi, "Image Steganography Techniques :an Overview'', International Journal of Computer Science and Security(IJCSS), vol 6, 2012.

[26] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, vol. 90, issue 3, p.p. 727-752, march 2010.