SECURE DATA TRANSMISSION USING IMAGE STEGANOGRAPHY

ABSTRACT—Image steganography is a field of steganography where images are used to hide information. Nowadays with the increasing lack of security online it is important to have means to make our data safe. In this paper we propose a method to increase the security of our data by means of steganography. We use a sparse encoded matrix to encode our information such as the key and data and this helps to increase the security of the algorithm. On further inspection we can see that the algorithm gives great results and can be used for practical purposes.

Keywords—Cryptography, Encryption, Secret key, Cover image, Steganography, Sparse matrix.

I . INTRODUCTION

Over the years the lack of information security has led to leakage of private information. A lot of recent developments has happened in the field of cryptography. Still there has been no decrease in the rate of cyber crime.

Some of the recent developments in cryptography have seen modifications to older algorithms. For example was a modification of the Caesar Cipher algorithm and has been seen to increase the efficiency of the algorithm by enhancing the security without changing the speed too much of the algorithm.

There has been a shift from main stream cryptography to field such as lattice cryptography and elliptic cryptography. Lattice based cryptography is the utilization of conjectured hard problems on point lattices. This type of cryptography has been seen to increase the security of the standard cryptography algorithms and hence is being preferred. Cryptography has found applications in the wireless sensor domain. This helps to secure information over insecure media as the information gets transmitted. Although cryptography gives good strength to the algorithm there is still lot to be desired over the increasing lack of security provided.

Cryptography is the technique of keeping information secured by converting text of one form into another. When somebody sees this new form of text it raises a doubt in their eyes and hence the evolution of steganography. Steganography helps to keep the information secure whilst at the same time preventing the knowledge of information being hidden from being leaked.

However latest developments give some positive hope with regards to cryptography being strong enough by itself .

Recently the strongest cryptography algorithm was broken down by means of a super computer. So there is still some time for cryptography to show it can be used as the sole form of security.

Latest research shows the development of leakage resistant algorithms. They solve the issue of leakage itself instead of making the algorithm stronger. This way the security is enhanced as the leakage of information is much harder for anybody to crack.

The rest of the paper is organized as: Related work (which talks about recent developments in the field of steganography and how those developments have helped to strengthen security), Proposed work (which gives an explanation of the proposed algorithm and the steps involved in making it), experimental analysis (which gives a comparative analysis of the algorithm with the likes of the least significant bit algorithm among others, LSB is used because it is the most popular algorithm around for image steganogrpahy) and the conclusion of the proposed work.

II . EXISTING WORK

Steganography is a technique of hiding information where the idea that information is being hidden is not known to any eavesdropped no matter how smart he may be.

Some simple steganography algorithms include the use of facebook to hide information . In this they use cover images of a person to hide information and share it with particular set of people. This is very hard to identify as the fact that information is being hidden is known only to the people who are sharing that image with each other. Also facebook provides additional security information to prevent strangers from seeing your photos and this adds to the security of using facebook as a medium.

Another method to increase security of steganographic methods is to make your algorithm more random as it will increase the chaos factor of the algorithm. Breaking down of text into blocks and sending them in random order helps to increase the chaos factor due to the random nature of sending of the blocks. Sometimes using cryptography with steganography has been seen to increase the security of the algorithms. Many such methods have been proposed. In DWT was used with Lorenz encryption and visual cryptology. This gave 3 layers of security to the proposed algorithm and made it very difficult to crack down.

A universal function was developed in that gave distortion in a random or arbitrary domain and this caused to increase the security of the algorithm. Results showed that the algorithm did better than most recent algorithms.

In an algorithm was developed which was content adaptive i.e the algorithm adapted on the basis of the proposed content. This was done along with decreasing statistically detectability and the results showed great increase in security. This is considered one of the state of the art approaches to steganography.

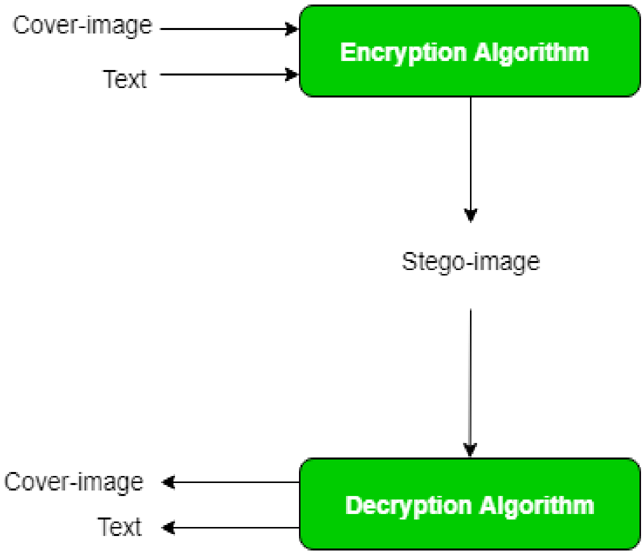
In the use of universal distortion was proposed and it was seen that the algorithm gave great results.

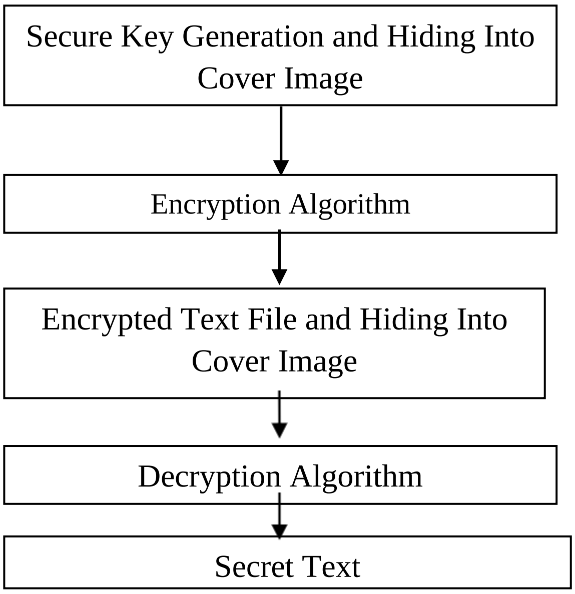
Another algorithm that used combination of Cryptography and steganography algorithms was proposed in. Here the use of blowfish algorithm increased the security of the information before even hiding it actually.

In the authors proposed content adaptive pentary steganography algorithm that used multivariate generalized Gaussian cover model to execute. Again since this was a content adaptive algorithm it gave great results in terms of execution and accuracy.

III . PROPOSED METHOD

An image is represented as N*M*3 (in case of color images) matrix in memory, with each entry representing the intensity value of a pixel. In image steganography, a message is embedded into an image by altering the values of some pixels, which are chosen by an encryption algorithm. The recipient of the image must be aware of the same algorithm in order to known which pixels he or she must select to extract the message.




Secure Key Generation and Hiding Into Cover Image
Encryption Algorithm
Encrypted Text File and Hiding Into Cover Image
Decryption Algorithm
Secret Text

ENCRYPTION SIDE:

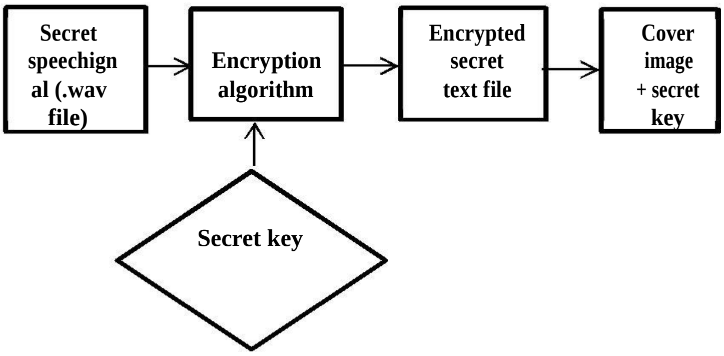


Fig. 1. Encryption at transmitter end

ALGORITHM:

1. For each character in the data, its ASCII value is taken and converted into 8-bit binary .
2. Three pixels are read at a time having a total of 3*3=9 RGB values. The first eight RGB values are used to store one character that is converted into an 8-bit binary.
3. The corresponding RGB value and binary data are compared. If the binary digit is 1 then the RGB value is converted to odd and, otherwise, even.
4. The ninth value determines if more pixels should be read or not. If there is more data to be read, i.e. encoded or decoded, then the ninth pixel changes to even. Otherwise, if we want to stop reading pixels further, then make it odd.

Repeat this process until all the data is encoded into the image.

DECRYPTION SIDE:

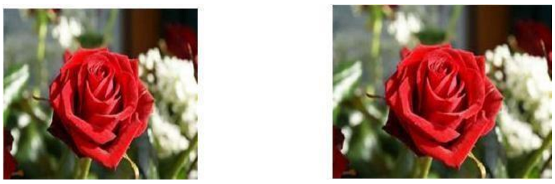
ALGORITHM:

For decoding, we shall try to find how to reverse the previous algorithm that we used to encode data.

1. Again, three pixels are read at a time. The first 8 RGB values give us information about the secret data, and the ninth value tells us whether to move forward or not.
2. For the first eight values, if the value is odd, then the binary bit is 1, otherwise it is 0.
3. The bits are concatenated to a string, and with every three pixels, we get a byte of secret data, which means one character.
4. Now, if the ninth value is even then we keep reading pixels three at a time, or otherwise, we stop.

IV. EXPERIMENTAL RESULTS:

The encrypted message with secret key generated also hidden into digital images . The secret key generated by secret key algorithm is again go through secret key hiding algorithm. The authorized person who know the key retrieval procedure able to retrieve the secret key. The position of key hiding is decided at transmitter end by the user . The secret key generated at transmitter end contains the name of noise hidden inside the encrypted speech signal.



The original image and steganographed image with encrypted secret speech file hide inside the cover image shown in Fig. 5. In the above case of both the images we find that both the original image and the steganographed image appears to the same without any modifications .Here it becomes difficult to identify whether any information has been hidden inside the image.

V. CONCLUSION

In this paper a robust encryption method to encrypt a secret text message inside cover image is developed. The secret key is generated within the encryption algorithm directly according to the entered numbers and letters at transmitter end. For the decryption of hidden file one has to go through 2512 combinations of characters and numbers which is very difficult for attackers to hack the secret data and if the password is entered incorrectly for consecutively 3 times then the entire message available to the hacker is deleted completely. Every time a new secret key will be generated though the same secret signal entered as the key developed is stored in the database and compared at transmitter end .Thus the secret data will be received by the authorized person at receiver end only when the secret key is entered correctly.

REFERENCES

[1] The IEEE database: cs.utdallas.edu/loizou/speech/noiseus

[2] http://www.pacdv.com/sounds/voices-2.html

[3] www.wavesource.com/people/men.htm

[4] Joyshree Nath, Sankar Das, Shalabh Agarwal, Asoke Nath, “A challenge in hiding encrypted message in LSB and LSB +1 bit positions in various cover files, ” Journal of global research in computer science, Vol. 2, No. 4, PP. 180-185, April 2011.

[5] Satyaki Roy, Joyshree Nath, A. K. Chaudhari, Navajit Maitra, Shalabh Agarwal, Asoke Nath, “Ultra Encryption Standard (UES) Version-IV : New Symmetric Key Cryptosystem with bit-level columnar Transposition and Reshuffling of bits,” International Journal of Computer Applications, Vol. 51, No. 1, PP. 28 -35, August 2012.

[6] Harjinder Kaur, Gianetan Singh Sekhon, “A four level speech signal encryption algorithm, ” IJCSC, Vol. 3, No. 1, PP. 151-153, January 2012.

[7] Divya Sharma, “Five level cryptography in speech processing using multi hash and repositioning of speech elements, ” International Journal of Engineering Technology and Advanced Engineering, Vol. 2, No. 5, PP. 21-26, 2012

[8] M. Nutzinger, “Real Time attacks on Audio Steganography, ” Journal of Information Hiding and Multimedia Signal Processing, Vol. 3, No. 1, PP. 47-65, 2012