StegoCrypt: Combining steganography and cryptography

Xi Yuan, Cai Peng

BUST, China

Abstract—**The utilization of pictures to conceal data is a highlight which leaves little uncertainty in a watcher's psyche. Utilizing any medium to shroud data alludes to a strategy called steganography. When we utilize a picture as a medium then that technique is called picture steganography. The most renowned technique to now is the Least Significant Bit Algorithm (LSB). In that technique, the least critical piece of every pixel is taken and data is covered up in that. This anyway is effectively brittle. Consequently an option and increasingly secure arrangement is given. First the information is scrambled utilizing the Blowfish calculation. Next an inventive technique is displayed. This encoded square is broken down to 'n' littler squares and 'n' pictures are picked indiscriminately what's more, each picture is made to conceal a square of the encoded information. To keep up the right arrangement of hinders a hash table is kept up. This is then encoded utilizing LSB to another picture called the hashing picture. This hashing picture is sent alongside the 'n' different pictures. To separate the information out, first the hash picture is acquired and utilizing this the scrambled square is reassembled and after that unique information is gotten by unscrambling.**

Keywords—steganography, blowfish, crytpography

I. Introduction

Steganography is something regularly confounded and misjudged with cryptography. Both, however are being utilized for a similar point, that is to shroud significant data. Anyway the distinction lying mostly with the way that in cryptography the aim is to make removing the information inconceivable, where as in steganography the primary point is to avoid any kind of assault. Cryptographic calculations give yield where the data can be seen in spite of the fact that encrpyted what's more, the nature of this yield would almost certainly cause an assault.

Steganographic calculations attempt to guarantee such assaults never occur by disguising the way that data is being covered up in any case. This paper will consolidate the advantages of the two kinds of calculations to fill the primary need: covering up of information. A few standard calculations are utilized and joined with an creative upgrade together to make a considerably more proficient calculation in itself.

First let us comprehend the renowned LSB calculation. To comprehend LSB calculation think about a model, a lattice for 3 pixels of a 24-piece picture can be as per the following: 00101101 00011100 11011100 10100110 11000100 00001100 11010010 10101101 01100011 When the number 200, which twofold portrayal is 11001000, is inserted into the least huge bits of this piece of the picture, the subsequent network is as per the following: 00101101 00011101 11011100 10100110 11000101 00001101 11010010 10101100 01100011.

The Blowfish encryption calculation is the most productive encryption calculation on the planet according to [1]. It produces scrambled data that is more diligently to unscramble than even the as of now most utilized calculation Advanced Encryption Standard [2].

II. Related Work

In [3] the creator oozes concealing a picture utilizing a surface as the medium spread picture. Since a surface is only a set of pixels that recurrent itself it winds up simpler to shroud information. Additionally since the surface could be spread to any ideal size, a lot bigger data could be covered up.

In [4] the creators use non-direct confused mapping. The information to be covered up is right off the bat made to insert onto a mixed picture. Simultaneously the picture utilized as spread is dependent upon Discrete Wavelet Transform. This yield picture is later inserted together with the mixed picture. This strategy can shroud huge measure of information, however should the guide utilized for mapping be gotten its amazingly simple to get the data.

In [5] the creators propose a strategy for concealing information utilizing any of the distinctive RGB shading channels. A picture has 3 channels, so changing any of the channel's doesn't essentially change the picture from a visual point of view. Anyway this technique can't be utilized for bigger pictures.

In [6] the creators propose different advances, first Huffman encoding is done on the information and the information is then separated to squares. At the same time Discrete Cosine Transform is performed on the spread picture. Least Significant Bit calculation is then altered utilizing the Huffman esteems gotten. Keeping up these Huffman codes is amazingly significant since loss of Huffman codes infers lost information.

Calculation time for this strategy is additionally generally enormous. In [7] twofold layer of security is given to the information, the first layer is utilizing the standard Least Significant Bit strategy and the subsequent layer includes utilizing the Data Encryption Standard Calculation. Steganography doesn't supplant the encryption of information, rather it gives an additional security highlight to the information. This expands the security of the information as the content is presently scrambled too.

In [8] the message wanted to be covered up is inserted in just the blue piece of the RGB channel. Results demonstrated that this upgraded the security level of the picture as visual contortion was not noticeable.

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

In [9] the mystery information is taken and from the outset it is shrouded utilizing the Vigenere encryption strategy to expand the standard of security of the information. Next the Lempel Ziv Welch (LZW) strategy is utilized to pack the information to shroud its genuine limit. Subsequently, the all-encompassing knight visit calculation is actualized where each piece stream of the information is made to spread out on the picture. This upgrades the strength of the picture.

In [10], a steganography calculation dependent on discrete cosine change, Arnold Transform, Chaotic System is delineated. The framework creates a novel arbitrary arrangement for spreading information in the recurrence band, Discrete Cosine Change coefficient of the spread picture. The mystery information is at that point mixed by using the Arnold Cat Map which upgrades the security highlight. The recuperation procedure is finished by rehashing the technique in turn around. Some other recent work can be seen in [11-15].

III. PROPOSED ALGORITHM

From the outset the client takes the content to be covered up and afterward encodes it by utilizing the Blowfish encryption calculation with the assistance of a key that is variable long. The key will be chosen by the client.

This scrambled data is then made to break to 'n' squares. Presently 'n+1' pictures are chosen indiscriminately from a lot of 'm' pictures where 'm'>'n'. Each messed up square is scrambled at arbitrary to one picture. A hash table is kept up to get a right request regarding grouping of information.

This hash table and every one of the squares are then implanted into the 'n+1' pictures utilizing LSB calculation. These 'n+1' pictures are then sent. At the collectors side the 'n+1' pictures are acquired. The collector at that point acquires the hash picture first.

The data with respect to position of the hash picture is known previously hand to the collector. Utilizing the hash picture he removes the right arrangement of information. He at that point unscrambles it utilizing the key which is likewise part of the hash table. The whole calculation is executed in Python utilizing OpenCV.

The benefits of the proposed strategy are various. Right off the bat the encryption improves the security. At that point the irregularity of the sending of pictures further improves the security of the calculation.

Additionally it tends to be seen later in the results that as far as time of execution the proposed calculation isn't critical.

The reason for concealing data safely is finished flawlessly. The significant thing to be done is the pictures picked ought not be rehashed, anyway for the situation they are rehashed the names of the pictures are changed by hard coding to guarantee the framework doesn't get confounded.

Additionally in examination with latest work as far as picture steganography, the proposed calculation gives superb results and takes generally lesser time and gives generally secure results. Consequently the proposed calculation can be proposed to be utilized as a standard calculation. Figure 1 portrays the progression of the work.

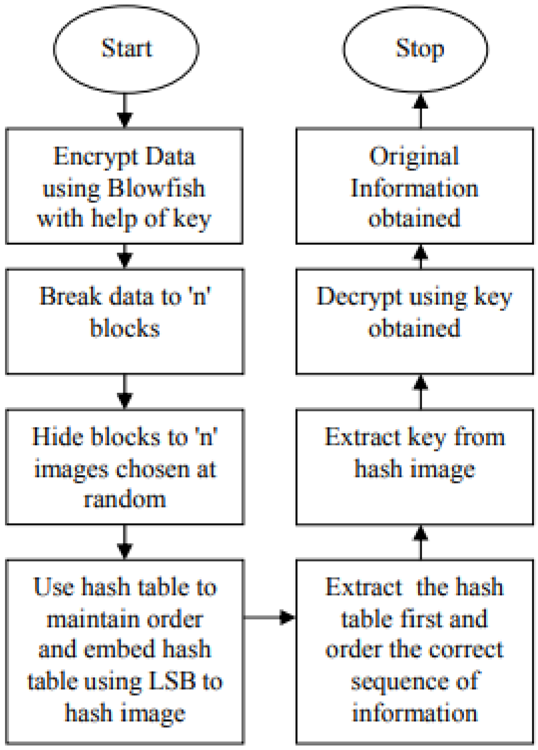

Start
Encrypt Data using Blowfish with help of key
Break data to 'n' blocks
Hide blocks to 'n' images chosen at random
Use hash table to maintain order and embed hash table using LSB to hash image
Extract the hash table first and order the correct sequence of information
Extract key from hash image
Decrypt using key obtained
Original Information obtained
Stop

Fig. 1. Flowchart of Proposed Method

IV. RESULTS

To test the quality of the calculation following tests were done in contrast with the standard Least Significant Bit Calculation,

1) decide most extreme size of record that can be covered up

2) time that is required for execution of the two calculations

3) Peak Signal To Noise Ratio for unique to new picture

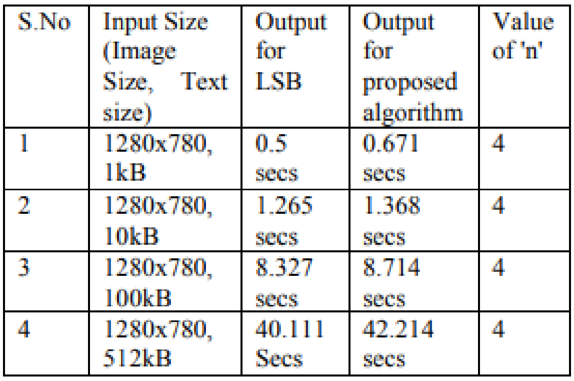
Table I demonstrates the outcomes for a progression of tests done to decide the greatest size of a book record that could be concealed utilizing the two calculations. As can be seen from results, both give a similar yield.

Table I. Result for determining maximum size that can be hidden

S.No	Input Size	Output for LSB	Output for proposed algorithm	Value of 'n'
1	320x240	512kB	2048kB	4
2	1280x780	2MB	8MB	4

Table II delineates the outcomes for the trial directed to decide the time required for execution of the calculation in examination with the standard LSB calculation. As anyone might imagine seen from the table time taken to execute the standard LSB is lesser. This is normal, since we are joining encryption to the proposed calculation alongside the additional component of breaking to squares and the arrangement of hash table, which all add to the multifaceted nature to execute the program and subsequently will unquestionably lead to an expanded yield as far as time of execution. Still the ideal opportunity for execution as can be seen isn't too huge moderately. Additionally as a rule documents of size at any rate 1 MB are taken to be shrouded which gives a significantly littler contrast for yield.

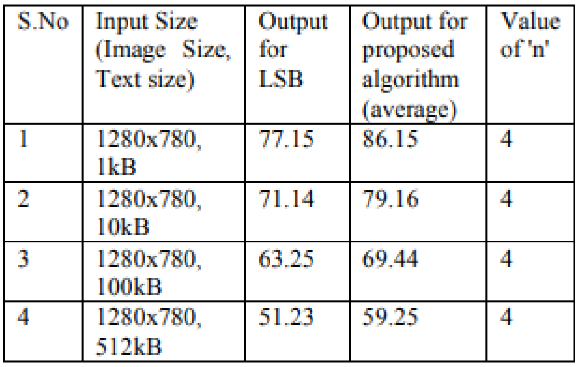
Table II. Time of execution



S.No	Input Size (Image Size, Text size)	Output for LSB	Output for proposed algorithm	Value of 'n'
1	1280x780, 1kB	0.5 secs	0.671 secs	4
2	1280x780, 10kB	1.265 secs	1.368 secs	4
3	1280x780, 100kB	8.327 secs	8.714 secs	4
4	1280x780, 512kB	40.111 Secs	42.214 secs	4

Table III displays the consequences of Peak Signal to Noise Ratio between the pre-calculation picture and the post-calculation picture. The Mean Square Error (MSE) ,the Peak Signal to Noise Ratio (PSNR) are the two fundamental blunder measurements used to think about picture pressure quality. The MSE speaks to the aggregate squared mistake between the compacted and the unique picture, while PSNR speaks to a proportion of the crest mistake. This is utilized to demonstrate the most extreme contrast between the pictures. The Peak Signal to Noise Ratio is the distinction between comparing pixel estimations of the pre-calculation to post-calculation picture. This is finished utilizing MatLab. The higher the estimation of PSNR the lesser is the distinction in nature of the picture.

Table III. PSNR value determination



S.No	Input Size (Image Size, Text size)	Output for LSB	Output for proposed algorithm (average)	Value of 'n'
1	1280x780, 1kB	77.15	86.15	4
2	1280x780, 10kB	71.14	79.16	4
3	1280x780, 100kB	63.25	69.44	4
4	1280x780, 512kB	51.23	59.25	4

Following are the images before and after execution of the proposed algorithm. As can be seen, the difference is not visually perceptible.

V. CONCLUSION

A calculation has been recommended that essentially upgrades the security of the calculation. A creative upgrade is included terms of expanding the confusion factor of the calculation by adding the irregularity to it. Likewise it can be seen that the hour of execution doesn't get essentially fluctuate. This guarantees the calculation is as proficient as conceivable with respect to time and furthermore security.

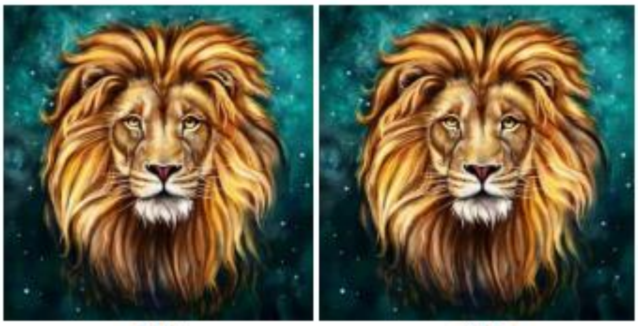
Following ends can be made based on the examination of the calculation.

- The proposed calculation expands the limit of concealing information since we utilize more pictures. This too expands the size of info we need. In any case, with extending innovation, size of information has halted being a noteworthy disadvantage for calculations.

- The proposed calculation sets aside somewhat more effort to execute than the standard LSB. This is normal as three extra highlights are added to the calculation to be specific: encryption utilizing Blowfish calculation, breaking of squares and arrangement of hash table. And still, at the end of the day for bigger records the time taken isn't critical.

- The proposed calculation, since it utilizes more pictures, utilizes lesser information per picture than the standard LSB what's more, consequently gives a higher PSNR esteem for each picture, which means the watcher will think that its harder to separate considerably more than the standard LSB. PSNR is frequently the most utilized distinctive factor to decide the quality of a steganography calculation.

- The most significant viewpoint here is that the LSB can be effectively decoded. By utilizing the proposed calculation it builds the security factor of the picture. The encryption improves the security and at that point the irregularity expands the disarray factor of the calculation.



2 (a) 2 (b)

Fig 2(a) Original Image (b) Output Image

REFERENCES

[1] Gowda, S.N., 2016, September. Innovative enhancement of the Caesar cipher algorithm for cryptography. In 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Fall) (pp. 1-4). IEEE.

[2] Babu, K Ravindra, S U Kumar, and A V Babu. "A Survey on cryptography and Steganography methods for information security." International Journal of Computer Applications Volume 12 Issue 3 pp 13-17, December 2010.

[3] K Wu and C Wang, “Steganography using reversible texture synthesis” IEEE Transactions on Image Processing Vol.24 pp 130-139,January 2015.

[4] Gowda, S.N., 2016, October. Using Blowfish encryption to enhance security feature of an image. In 2016 6th International Conference on Information Communication and Management (ICICM) (pp. 126-129). IEEE.

[5] M T Parvez and A Gutub, “RGB Intensity Based Variablr-Bits Image Steganography”, IEEE Asia-Pacific Services Computing Conference, pp 1322-1326, December 2008.

[6] A Nag, S Biswas, D Sarkar, P P Sarkar “A novel technique for image steganography based on Block-DCT and Huffman Encoding” International Journal Of Computer Science and Information Technology, pp 103-112, vol 2, June 2010.

[7] Gowda, S.N. and Sulakhe, S., 2016, April. Block Based Least Significant Bit Algorithm For Image Steganography. In Annual Int'l Conference on Intelligent Computing, Computer Science & Information Systems (ICCSIS-16) (pp. 16-19).

[8] S Gupta , G Gujral and N Aggarwal "Enhanced Least Significant Bit algorithm For Image Steganography" IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, pp 40-42, July 2012.

[9] Gowda, S.N., 2016, July. Dual layered secure algorithm for image steganography. In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (pp. 22-24). IEEE.

[10] Gowda, S.N., 2016, November. An advanced Diffie-Hellman approach to image steganography. In 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 1-4). IEEE.

[11] M Bashardoost ,G B Sulongand, P Gerami "Enhanced LSB Image Steganography Method By Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, pp. 221-227, March 2013.

[12] S Singh and T J Siddiqui "A Security Enhanced Robust Steganography Algorithm for Data Hiding" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, pp 131-139, May 2012.

[13] Gowda, S.N., 2016, December. Advanced dual layered encryption for block based approach to image steganography. In 2016 International Conference on Computing, Analytics and Security Trends (CAST) (pp. 250-254). IEEE.

[14] Gowda, S.N. and Vrishabh, D.N., 2017, April. A secure trigonometry based cryptography algorithm. In 2017 International Conference on Communication and Signal Processing (ICCSP) (pp. 0106-0109). IEEE.

[15] Gowda, S.N., 2017, July. An intelligent fibonacci approach to image steganography. In 2017 IEEE Region 10 Symposium (TENSYMP) (pp. 1-4). IEEE.