e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

SEARCHING FOR STEGO KEY AND ITS VARIOUS METHODS

Nikita Rabade*1, Dr. Y.S. Thakur*2

*1,2Department Of Electronics And Communication Engineering, Ujjain Engineering College Ujjain, India.

ABSTRACT

In the broadest sense, steganalysis entails recognising suspicious items initially, followed by additional analysis in which we seek to recognise the steganographic technique applied for embedding, recover the stego key, and ultimately extract the secret message. This article outlines a method for locating the stego key in key-dependent Sterographic techniques in the past, stego key searches were conducted using laborious searches to hunt for recognised structures (such headers) in the extracted bit-stream. If the message is encrypted, the search becomes much more expensive because all possible encryption keys must be tested for each stego key.

In this paper, we show that the complexity of the stego key search is determined solely by the size of the stego key space and is independent of the encryption algorithm for a wide range of steganographic schemes. An exhaustive stego key search can be used to determine the correct stego key by quantifying statistical properties of samples along portions of the embedding path.

Keywords: Forensic, Steganography, Steganalysis, Stego Key.

I. INTRODUCTION

Steganography is a method of concealing communication by encoding data into seemingly unimportant cover items, such digital photographs. The embedding process slightly modifies the original picture, also known as the cover image, to create the stego image, which can house a hidden message. A secret stego key may be required for the embedding procedure. The stego key is used to manage the embedding procedure, including the choice of message-carrying pixels or coefficients, etc. The message is often pre-pended with a header before being embedded, after which it is further compressed and/or encrypted using an encryption technique with the encryption key.

II. SEARCHING FOR STEGO KEY

One strategy for the stego key search would be to first determine which samples have been altered before attempting to decipher the PRNG that produced the embedding route. This strategy, nevertheless, is impossible for a number of reasons. Secondly, it might be quite challenging to tell whether samples have been altered in general.

Second, because on average 50% of samples were not modified because their parity already matched the message bit, even if we were able to identify the modified samples, we would not be able to determine the sequence in which they were modified or the whole path. Thirdly, it is highly challenging to reverse-engineer the majority of PRNG in the sense of separating the seed from the PRN sequence.

To minimise any misunderstanding, we have refined the stego key search. The steganographic algorithm may use a many-to-one mapping (e.g., a hash function) to map the user pass (or password) to the PRNG seed. As a result, identifying the user password via any search engine may be impossible. method. So, when we speak of looking for the stego key in this work, we are really looking for the seed that was used to initialise the PRNG rather than the user pass. In other words, if our search is successful, we will be able to locate the proper seed, embedding path, and extract the embedded bits even if we are unable to retrieve the embedded bits.

Now it's time to go through the fundamentals of our stego key search strategy. Let N samples xi, i1,..., N=I represent the cover picture X. The samples xi might be different colours depending on the picture format.

Grayscale, colour indices, and DCT coefficients are all examples. Let K represent the space of all potential stego keys that lead to various pseudorandom pathways. The stego picture S=si is obtained after inserting the message. mN samples in X are visited (and perhaps changed) along the route produced by the stego key K0K during embedding. With only the stego picture, our aim is to identify the embedding key K0. The following is how we continue.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

To increase the SNR between the cover picture and the stego signal, we can first filter the stego image.

The stego picture samples will also be decorrelated by the filtering. This first step can significantly enhance the stego key search's performance17, particularly for stego schemes that operate in the spatial realm. We skip this step for JPEG pictures since the individual DCT coefficients already have weak inter-block correlations.

Let I(j) stand for the collection of sample indices visited along the path derived from each key KjK.

Provided the message included within the picture is a random binary stream, on average 50% of the samples in the sequence siiI (0) will already have the right parity, and 50% of them will have had their parity changed as a result of the embedding procedure.

As a result, n distributions were calculated using the first n samples along the wrong pathways, siiI(j), j>0.

The samples' Probability Density Function (PDF), which models them as realisations of an i.i.d. random variable, provides a comprehensive statistical description of them. In order to get the proper key, one should look for samples that have a "outlier distribution." We test it to find the outlier distribution.

The density of embedding adjustments over the whole picture is the same as along an improper path, assuming that the embedding changes are randomly distributed throughout the stego image. In order to find the predicted distribution of n samples si along a path created from an invalid key, the PDF h of samples si may be calculated. based on the entire stego picture (total of N samples). The samples siiI(j) are then tested to see if they were obtained from h for each key. We use non-parametric statistical tests, such the chi-square test, for this purpose.

III. STEGO KEY SEARCH FOR IMAGES

The suggested strategy aims to establish a reliable and safe method of message transfer so that sensitive and private data can be delivered over the network in a protected way without being exposed to any assaults from an unintended receiver. * The suggested technique works for grayscale photos. The 7th bit of each pixel is subjected to a mathematical operation, and on the basis of a combination of these two values, 2 bits of the message may be recovered from each pixel. *e 7th bits of the selected pixel and pixel + 1 value are extracted. There are four potential pairings: 00, 01, 10, and 11. several benefits, including the ability to store two bits of information per message There can be a maximum change of +2 and 2 in the 8th bit for each pixel and the approach is not dependent on it. pixel value when entering the data into the picture file. *This approach significantly improves upon steganography's limitations.

IV. HISTOGRAM RESULTS FOR THE IMAGES

Using the suggested approach and a message size of 2 KB, the histogram results of a few photographs are shown. The corresponding histograms for the original image, the stego image, and both are presented.

The Proposed Image Steganographic Algorithm

The suggested method, its embedding and extraction procedures, and MLEA are all shown in this section. According to Fig., the suggested steganographic technique is divided into three phases: encryption, data mapping, and extraction. These three stages are combined to create a sophisticated steganographic system with several degrees of protection.

Mathematical Modeling of Proposed Scheme

Let's say M represents the hidden message that has to be included in the carrier picture (C).

S is the stego picture, K is the secret key, and T displays the transposed image. According to equations 1 through 3, the embedding process uses the three functions

$$T = \alpha(C) \quad (1)$$

$$M' = \beta(M,K) \quad (2)$$

$$S = \gamma(T,M') \quad (3)$$

The first function returns T, the transposed picture, from an input of C.

After using MLEA on message M with secret key K, M' is the final encrypted message produced by second function. The third function, which uses the suggested steganographic technique, creates the stego picture S after concealing the encrypted message M' in the transposed image T.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

The recipient has to apply the reverse operations in order to extract the original hidden information. The following three functions are used for extracting the actual message as described in equations 4-6.

$$T = \alpha^{-1}(S) \quad (4)$$

$$M' = \Upsilon^{-1}(T) \quad (5)$$

$$M = \beta^{-1}(M', K) \quad (6)$$

In extraction process, function applies transposition on stego image S and returns T which is the resultant transposed image. Using eq. 5, the encrypted secret message M' is extracted from the image T by applying the extraction algorithm. At the end, original message M is achieved by using eq. 6 when encrypted message M' is decrypted by function using secret key K.

Experiment

Via a number of test photos, the performance of the planned work is assessed in this part. Although a collection of standard greyscale photos is used to guarantee the efficiency of the recommended work, we have published findings for four standard greyscale photographs as a handy reference in this study. The test images are chosen with consideration of various image features to estimate their performance in terms of visual quality and capacity/payload of stego-images.

With stego-images having a large payload or capacity, we were able to get strong PSNR values. The distortion that resulted from embedding the secret message into the cover picture is therefore relatively reduced and invisible to HVP in our approach, according to the PSNR values as well as the visual look of the stego-image and histogram. Based on the above equation, the PSNR value is calculated.

$$PSNR = 10*\log10\left(\frac{255^2}{MSE}\right)dB \quad \ldots\ldots\ldots\ldots(7)$$

where MSE is the mean square error between the cover image and stego-image. The MSE is computed using the following equation (2)

$$MSE = \frac{1}{M * N}\sum_{i=0}^{M-1}\sum_{j=0}^{n-1}(Is(i,j) - Ic(i,j)^2$$

where M and N represent the width and height of IS stego-image and IC is the cover image.

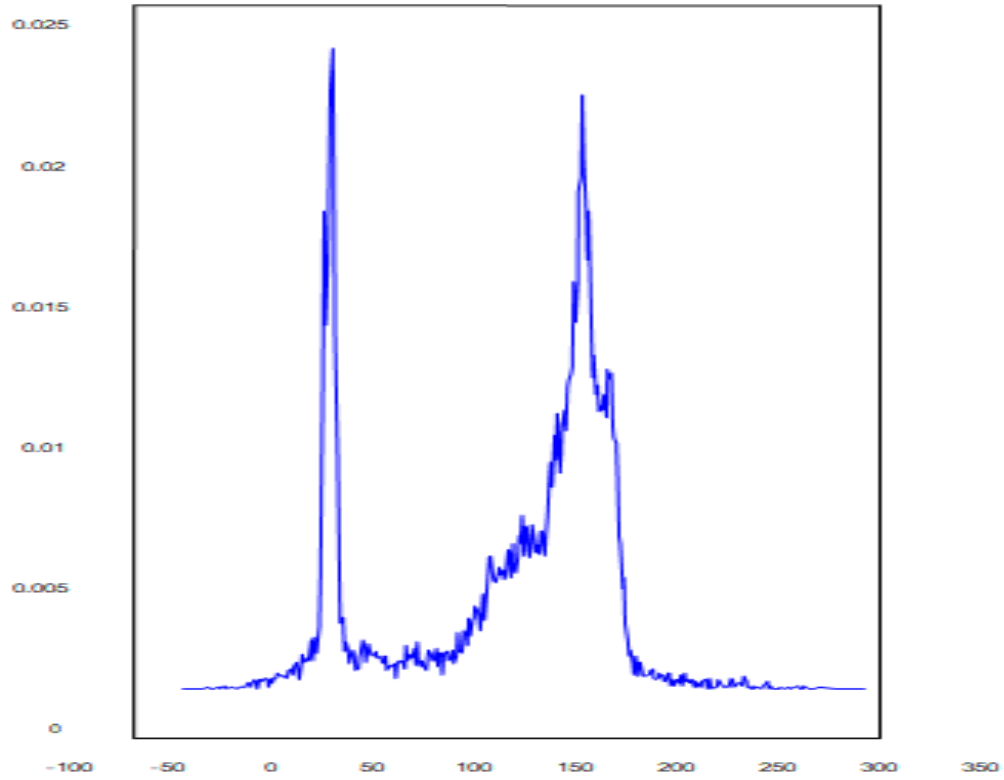
V. WAVELET CODING DESIGN

In recent years, wavelet image coding has been a fascinating and fruitful field of research in the image processing community, especially in connection to the results of image compression, but it is also appropriate for progressive transmission and offers a multi-resolution capacity. Although it may eliminate some redundancy and decorrelate the neighbouring pixels, applying the wavelet transform on pictures for compression alone does not result in a reduction in the quantity of data to be reduced. Quantizing the transformed coefficients is a typical technique for lowering the number of bits needed for compression. where progress was made without the use of unnecessary information. This method is especially suitable for critical applications, such as client/server communication, where the client may select the actual compression ratio and compress images at a certain target rate.

Wavelet Coefficients Encoding : Depending on the amount of decomposition, the wavelet transform divides the input picture into low-frequency coefficients, also known as coarse bands, and a number of high-frequency bands, also known as detail signals. Both the low pass and high pass versions of the original image may be viewed in these findings. the probability distribution of the high band coefficients, which resembles laplacian features with a mean of zero. The coefficients produced by the wavelet transform are also substantially less correlated than those of the original pictures and are simpler to code. Also, it can be seen that all of the identical position bands, including those that are diagonal to diagonal and horizontal to horizontal, appear like scaled-down replicas of one another. It should be noticed, too, that the bulk of the energy in the high bands is more or less concentrated close to regions that correlate to edge activity in the original picture. According to this, regions that hold the majority of the information should be encoded more accurately than the remainder. In order to compress images, a wavelet transform must be used in conjunction with another coefficient coding

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:03/March-2023 Impact Factor- 7.868 www.irjmets.com

method. In reality, the idea behind wavelet coefficient compression is that high-resolution features are less noticeable to the human eye and may thus be rebuilt with less processing.



Wavelet Coefficients of low band

Wavelet Transform combined with Scalar Quantisation (SQ) and Vector Quantisation (VQ) have led to numerous schemes for image data compression [2, 4, 5, 6, 9, 13] using a multiresolution and pyramid algorithm [10, 12, 14, 15] the wavelet transform organizes the coefficients to enable effective SQ and VQ encoding. Both approaches have their own advantages and disadvantages. It is known that thehigh frequency coefficients can be modelled fairly. Scalar quantisation takes advantage of this fact for the design of their quantisation table. On the other hand, it is known that sharp edges are characterised byfrequency components of all resolution. Hence, there will be some residual correlation between coefficients of different scales. Vector quantisation exploits the correlation among coefficients of different scales.

Wavelet Scalar Quantisation

This approach checks the input data or picture value element by element with the quantiser's judgement levels. The receiver receives an index indicating which quantisation interval is appropriate, and the receiver reconstructs an approximation to the associated level. Until date, one of the successful wavelets was employing scalar quantisation, and the first people to do so were Gharvi and Tabatabi. They used the two-level wavelet transform, with the lowest resolution coded using Differential Pulse Code Modulation (DPCM) and a non-uniform scalar quantiser, then variable length coding. They used the two-level wavelet transform, with the lowest resolution coded using Differential Pulse Code Modulation (DPCM) and a non-uniform scalar quantiser, then variable length coding. The remaining bands are coded using PCM with a consistent quantiser and run length coding. The Federal Bureau of Investigation (FBI) has adopted a standard for fingerprint image reduction [3, 7].

The bit allocation mechanism is used in Wavelet-Scalar Quantisation (WSQ). Each sub band has a unique quantisation step that is dictated by the subband's energy.

VI. PARITY CODING

Parity coding is a reliable audio Steganographic method. Rather of dividing a signal into individual samples, this approach divides the original signal into distinct samples and embeds each bit of the secret message from a

parity bit. If the parity bit of a chosen area does not match the secret bit to be encoded, the procedure inverts the LSB of one of the region's samples. As a result, the sender has additional options for encoding the secret bit.

Considering Parity method uses LSB coding technique for data hiding in audio. However, instead of directly replacing LSBs of digitized samples with the message bits, it first checks the parity of the samples and then carries out data embedding. Using XORing of LSB's method performs XOR operation on the LSBs and then depending on the result of XOR operation and the message bit to be embedded, the LSB of the sample is modified or kept unchanged. The method described below performs XOR operation on first 2 LSBs. The XORing can be further expanded to 3 LSBs, 4 LSBs upto 16 LSBs so as to increase the level of encryption. From experimental results, it is seen that the proposed methods are effective. From listening tests, no difference is found between the original audio signal and the stego audio signal. The hidden information is recovered without any error. Also, this approach increases the capacity of the cover audio by as much as 8 times and provides robust encryption.

Echo Data Hiding

Echo data hiding is the process of embedding text (or data) in an audio recording by adding an echo to the original signal. The data is then obscured by altering three parameters of and then modulating with a pseudorandom signal and interleaving it with the cover-signal. Schemes for hopping frequencies. The frequency spectrum of audio files is altered in frequency-hopping SS such that it jumps between frequencies quickly.

VII. CONCLUSION

This review study looked into numerous stego key And Various Stenography Techniques. The fundamental ideas of stego key for images were discussed, as well as some current techniques such as Wavelet Coding Design and Parity Coding. key-dependent steganographic techniques have a way for determining the stego key.The search would become far more costly if the message were encrypted, as every stego key would need to be verified against every conceivable encryption key. In this research, we

VIII. REFERENCES

[1] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[2] Sridevi R., Damodaram A., SVL.Narasimham, Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security, Journal of Theoretical and Applied Information Technology, 2009.

[3] G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.Berglund, J.F. and K.H. Hofmann, 1967. Compact semitopological semigroups and weakly almost periodic functions. Lecture Notes in Mathematics, No. 42, Springer-Verlag, Berlin-New York.

[4] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, An introduction to steganography methods, World Applied Programming, Vol (1), No (3), August 2011. 191-195.

[5] Bender W, Gruhl D & Morimoto N (1996) Techniques for data hiding. IBM Systems Journal 35(3): p 313–336.

[6] Nedeljko Cvej, Algorithms for audio watermarking and steganography, Oulu 2004, ISBN: 9514273842.

[7] Sos S. Agaian, David Akopian, Sunil A. D'Souza1, Two algorithms in digital audio steganography using quantized frequency domain embedding and reversible integer transforms, USA.

[8] "audio steg: methods", Internet publication on www.snotmonkey.com

[9] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, "A Tutorial Review on Steganography".

[10] Beixing Deng, Jie Tan, Bo Yang, Xing Li, A Novel Steganography Method Based on Modifying Quantized Spectrum Values of MPEG/Audio Layer III, Proceedings of the 7th WSEAS International Conference on Applied Informatics and Communications, Athens, Greece, August 24- 26, 2007.

[11] Alaa Ismat Al-Attili, Osamah Abdulgader Al-Rababah, New technique for hiding data in audio file, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.7, July 2010.

[12] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, Information Hiding in Audio Signals, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010.

[13] Mazdak Zamani, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah, A Genetic-Algorithm-Based Approach for Audio Steganography World Academy of Science, Engineering and Technology 54 2009.

[14] Nedeljko Cvejic, Tapio Seppänen, Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04).

[15] Ajay.B.Gadicha1, Audio Wave Steganography, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume1, Issue-5, November 2011.

[16] R.J. Anderson and F.A.P. Petitcolas, "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and Privacy Protection, vol. 16(4), pp. 474–481, 1998.

[17] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB Steganography in Color and Gray-Scale Images", Magazine of IEEE Multimedia, Special Issue on Security, October-November issue, pp. 22–28, 2001.

[18] S. Dumitrescu, Wu Xiaolin, and Z. Wang, "Detection of LSB Steganography via Sample Pair Analysis", In: LNCS, vol. 2578, Springer-Verlag, New York, pp. 355–372, 2002.

[19] T. Zhang and X. Ping, "A New Approach to Reliable Detection of LSB Steganography in Natural Images", Signal Processing, vol. 83, No. 10, pp. 2085–2094, 2003.

[20] H. Farid and L. Siwei, "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines", In: LNCS, vol. 2578, Springer-Verlag, New York, pp. 340–354, 2003.

[21] J.J. Harmsen and W.A. Pearlman, "Steganalysis of Additive Noise Modelable Information Hiding", Proc. EI SPIE Electronic Imaging, Santa Clara, January 21–24, pp. 131–142, 2003.

[22] R. Tzschoppe, R. Bäuml, J.B. Huber, and A. Kaup, "Steganographic System based on Higher-Order Statistics", Proc. EI SPIE Electronic Imaging, Santa Clara, January 21–24, pp. 156–166, 2003.

[23] N. Provos and P. Honeyman, "Detecting Steganographic Content on the Internet", CITI Technical Report 01- 11, 2001.