Trigonometric Abstraction Based Variable Harmonic Sampling and Dual Encryption Steganography

Rajib Biswas, Gaurav Dutta Chowdhury, Samir Kumar Bandhyopadhyay

Abstract— In this paper, we have explored a new realm in image steganography centered around trigonometric analysis , multi-level varied encryption and differential embedding. To allow better harmonics in the stego – image sinusoidal referential curves have been intricately associated with pixel selection , optimization of sampling , and two – way varied embedding. Fragmentation of the secret data into sine and cosine curves have been deftly realized as variable functions of the steg – key and the secret data. The keen association of the image, secret data and steg - key, varied with a pixel dependant embedding results in a highly secure, reliable L.S.B.substitution. Meticulous statistical analysis have been provided to emphasize the strong immunity of the algorithm to the various steganalysis methods in the later sections of the paper.

Index Terms— Steganography, Steganalysis. Pixel, Sampling, Encryption, Decryption, Image, Steg key, LSB Substitution .

1 Introduction

THE sole role of steganography is to conceal the fact that any communication is taking place. Secret messages are embedded in cover objects to form stego objects. These stego objects are transmitted through the insecure channel. Cover objects may take the form of any irrelevant / redundant digital image, audio, video and other computer files.
In secure transmission of the stego objects without suspicious lies the success of steganography. Staganalysis methods aim at estimating retrieval of potentially hidden information with little or no knowledge about the steganographic algorithm or its parameters.

2 Literature Study

An extensive study of the related papers [1],[2],[3],[4] has given shape to this concept. We have meticulously analyzed the possibilities in the sphere of maximizing randomization , minimizing deviations and structuring strong coherence among the working sets. This paper is aimed at further increasing the equalization and reliability of the substitution based steganography [3] from its referrals by inducing strong coherence with the keen association of trigonometric curves and functions.

- *Rajib Biswas , Assistant Proessor in Heritage Institute of Technology,Kolkata-700107,India, rajib.biswas@heritageit.edu .*
- *Gaurav Dutta Chowdhury final year Student of Computer Science and Engineering inPailan College of Management and Technology, India, gauravduttachowdhury@gmail.com.*
- *Samir Kumar Bandyopadhyay Professor inDepartment of Computer Science and Engineering,University of Calcutta,Kolkata-700009, India. skb1@vsnl.com*

3 Our Proposed Method

In our method we have mainly four components as sampling, encryption , embedding and decryption. Sampling plays a key role here in our procedure, it involves the homogeneous and harmonic-based selection of pixels for encryption which strengthen the uniformity of the steganography procedure.

We have implemented a two – way variable encryption revolving around trigonometric functions of steg–key, secret data and the image .We then intend embedding the encrypted data in the sampled pixels, using a strong and efficient method , realizing the equalization of the sampled pixels with another set of variably generated samples. Subsequently , we use the decryption method to retrieve the image in the receiver end.

3.1 Sampling

Sampling is intricately associated with successful steganography and plays a central role in the process. In this paper, we have explored a highly secure and weight balanced algorithm to obtain variable samples spread equally throughout the cover image.
This papers explores a highly secure method of image steganography. The samples are selected based on the input cover object, secret massage and the steg key. Further, a striking feature of the sampling function is that the sample count decreases exponentially as we move inwards from the periphery to the centre of the picture. This is based on the idea that the centre of the picture is usually more meticulously noticed and focused on by the human eye, and peripheral parts generally attract lesser meticulous keen notice. The sampling is guided by variable selection of sampling algorithms parameterizing image and the steg–key. Harmonization of pixels have been meticulously observed through trigonometric analysis . The

sampling is strengthened keeping in mind the visible changes in the histogram, thereby repulsing steganalysis deftly. Further, the function ensures that approximately equal number of pixel samples have been selected from all four quadrants, to prevent clustering of samples from a single one.

Let P be the Steg key array and Pi be the ith position of the input steg key.
We generate an array Pass_val to obtain the phase values of the trigonometric curves as :
Pass_val[i]=func(Cycle- pass (P) , k)
Where k is a constant phase value dynamically set based on the input message.
Cycle- pass (P) cyclically generates the P elements until n(P) = n(0)
N = number of elements / characters
We compute the sample positions as :
Initially we convert the steg-key to a numeric array of range 0 to1.
Samp [i] = format (ASCII (Cycle- pass (P)) ,
where format (x) filters out a value in the range 0 and 1 from x.
We then intend applying trigonometric functions to compute another array as :

Samp_val[i] = tan (samp[i]).

Finally, we find the samples as :

Pixel_sel [i] = Samp_val[i] * width of the original image.

3.2 Encryption

We encrypt the secret message using a 2 – level encryption procedure . The first level of encryption is based on the secret message and steg-key. The second level of the encryption generates equalization samples from the image using trigonometric analysis and encrypts , parameterizing the intermediate message , harmonizing samples and the samples for encryption . We perform a steg- key based cyclic modification of the secret message followed by inter - operable second level encryption.

In the first level :

we compute the numerical difference in terms of the place values of the input message and the steg – key [5]. Thereafter, we use trigonometric functions to manipulate the numeric value as:

numval [i] = tan(Diff [i]).
where Diffadd gives the difference of place values. and

In the second level :
Next we implement another algorithm to draw the equalization samples from the image. We implement it as :

Samp_2 [i] = form (ASCII (Cycle- pass (P))
Where form s a function implemented to range the values of the array from 0 to 1.
Pixel_sel_2 [i] = func(steg-key, Samp_2 [i]).

Finally we do componential addition on the selected bits of the pixel in Pixel_sel [] array and the encrypted value numval to obtain the encrypted value as:

Enc_val [i] = com_add(Pixel_sel_2 [i] , numval [i]).

Now, we get an encrypted message Enc_val with the same number of elements as original message, which is all set to be sent through the insecure channel .

3.3 Embedding

In LSB based steganography [1], [2], [6], [7] the embedding of the encrypted message E in the selected sample pixel set S is done in a color-component varied bit encryption method.
Function RGB-image (RGB value) returns the maximum intensity color component, taking the pixel RGB value as parameter.
We extract from the selected pixel as follows :
Step 1 :
R -> red component value in the range of 0 – 256.
G -> green component value in the range of 0 – 256.
B -> blue component value in the range of 0 – 256.
Step 2 :
Convert the values to hexadecimal. Thus we get a MSB. and a LSB. value in the range of 0 – e.
Step 3 :
Convert the LSB hex value to decimal
Step 4 :
Convert the decimal value to ASCII
Step 5 :
The function max Intensify (R, G, B) is celled, which returns the colour component of maximum intensity.

Fig. 1. Cover image

Step 6 :

TABLE 1
EMBEDDING FORMAT FOR 7 BITS

1	2	3	4	5	6	7
r1	r2	r3	b1	b2	g1	g2
r1	r2	b1	b2	b3	g1	g2
r1	r2	b1	b2	g1	g2	g3

The last 3 bits are encrypted from the maximum intensity color component[1] and the last 2 bits are essential for the other 2 component. Thus we get 7 bits as either

TABLE 2
ENCRIPTED ASCII BITS

e1	e2	e3	e4	e5	e6	e7

Step 7 :
The encrypted input E_i is converted into its ASCII as follows: Then it is mapped on to the selected pixel Si.
Step 8 :
The modified R,G,B LSB values are connected back to its decimal values, which are in turn converted into the R, G, B LSB modified hexadecimal values.

Fig. 2. Stego Image

Step 9 :
The combined R,G,B MSB and LSB values are merged together and converted to decimal values ranging from 0 – 256.
Step 10 :
The R, G, B values are merged into 1 single RGB value and the value is set as that modified RGB value in the selected pixel Si.

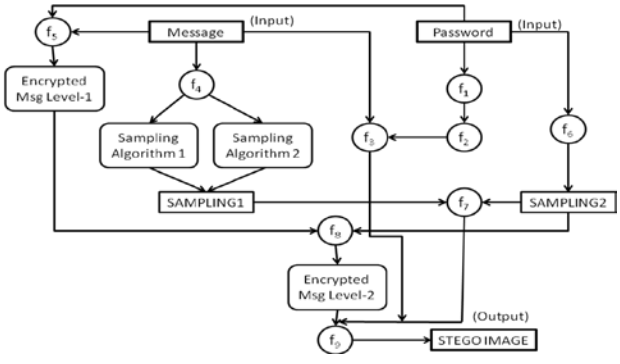

Fig. 3. Encryption , decryption flowchart.

The initial phase consists of retrieving the necessary information required for decoding from the corner pixels. In the first step we need to retrieve two important parameters from the encrypted image as secret message size and order of the stego images(incase of split and send algorithm).

Then we intend decoding the original message from the stego image and concatenate them in order to obtain the secret message. We first, apply the sampling algorithms to obtain the samples used for encoding. Then we proceed as below:
Step1:
We initiate by obtaining the two sample pixel arrays by the same algorithms we used previously. We then proceed by finding the maximum intensity color based on the sampling pixels obtained. After deducing the necessary embedding details , we then proceed to obtain the first level encrypted message by componential substraction as :
Numval[i] = comsub(Pixel_sel [i] - Pixel_sel_2 [i])
Where comsub is the componential subtraction performed on the intensity related bits for the individual components of the image.We induce a checking that if the value of Pixel_sel_2 [i] >Pixel_sel [i] we add a 1 before the obtaind L.S.B.'s and then substract to balance the adjustments done during encryption.
Diff [i] = tan-1(numval [i]).
The numerical difference between the original message and the Cycle_pass obtained from the steg – key at the reciever's end is thus obtained in the array Diff.
Step2:
We proceed to add the difference values to the corresponding subscripts to Cycle_pass to obtain the original message or part of the original message (in case of split and send) as :
O_i = Diff[i] + Cycle_pass[i].
Where O_i is the original message or a part of it.
We further use the order information embedded in the corner pixels to reassemble the fragments in order to form the complete message.

3.5 Split and Send

To remove the constraint of a fixed size secret message , we intent to put forward an automatic adjustment algorithm. This segment is mainly concerned with ensuring that input secret message size to be embedded bears a fairly reasonable ratio to the cover image size for which the distortion is negligible. The dynamic ratio value is defined depending on the dynamics of the image and the concentration of the color component values across the cross sections of the image. Based on the above concept , our algorithm warn against suspicion and suggests the use of another cover image or the copy of the same cover image, which can be generated automatically. On agreement we split the secret data in the best-proportion and the re-sample it. This process of splitting and re-sampling is a recursive process and terminates once an optimally permitted ratio is reached.
We store the necessary values required for decoding in the four corners of a picture.

4 Performance Analysis

It is indeed worth mentioning that trigonometric applications in image encryption and sampling have produced significant improvements in image harmonics and equalization. So much so, that the histograms show a remarkable response in regards to the curve statistics. We deployed the statistical studies to further clarify the proximity and negligible distortions produced in the stego image in the process of execution of the above proposed algorithms. From the table underneath it is noted that the statistical parameters like the MEAN, STANDARD DEVIATION and VARIANCE change only in their distant decimals thus proving its strong resistance to steganalysis.

Further, sharp transitions among adjacent pixels have been avoided. Analysis of correlational co-efficient(CC) [4] among

TABLE 3
MEAN, VARIANCE, STANDARD DEVIATION

Image / Statistical parameters	Original Image	Stego Image
MEAN	93.3847	93.3848
VARIANCE	2.9083e+003	2.9083e+003
STANDARD DEVIATION	53.9283	53.9285

the adjacent pixels show that there is a mass diffusion of statistical parameters in the stego image as compared to the original image.
The diffusion [3] is uniform throughout the encrypted image. The correlation decrease further with increase in the size of the secret message , although slightly and thus potent itself

TABLE 4
CO-RELATIONAL CO-EFFICIENT

CC / Image	Horizontal	Vertical	Left Diagonal	Right Diagonal
Original Image	0.0715	0.0456	0.0894	0.08864
Encrypted Image	0.0717	0.0452	0.0895	0.08862

against various statistical attacks.

5 Future Enhancement

This paper delves into the unexplored potential of trigonometric analysis in sampling , dual – layer encryption and componential embedding. The vast potential of trigonometric association in image encryption and sampling is yet to be realized, as we propose to bring further ideas on it under the scanner in our future endeavors.

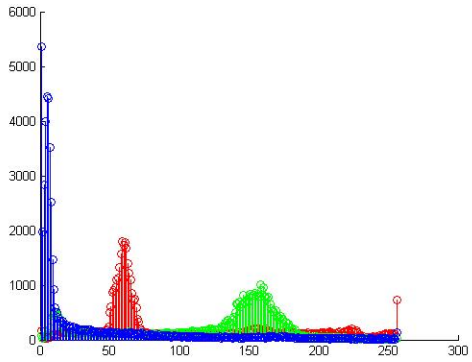

Fig. 4. Histogram of original image

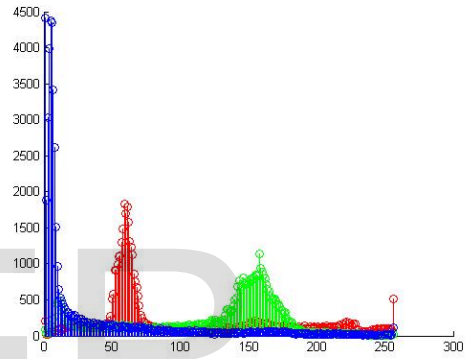

Fig. 5. Histogram of stego image

6 Conclusion

We conclude widening the window of image steganography through a realm of trigonometric applications and intensive improvisations done in almost all the processes of the evaluation.

Acknowledgement

The authors express their gratitude to all those who have in some way or the other been a part of this enterprise.

References

[1] RGB Intensity Based Variable-Bits Image Steganography by Mohammad Tanvir Parvez and Adnan-Aziz Gutub;ISBN – 978-0-7695-3473-2/08.

[2] Implementation of LSB Steganography and Its Evaluation for Various Bits by Deshpande Neeta,Kamalapur Snehal,Daisy Jacobs;

[3] Cover image preprocessing for more reliable LSB replacement steganography by Shreelekshmi R,M Wilscy,C E Veni Madhavan ;ISBN – 978-0-7695-3690-7,2010.

[4] A New Image Encryption and Steganography Scheme by Hongmei Tang,Gaochan Jin,Cuixia WU,Peijiao Song ; ISBN : 978-0-7695-3906-

5/09 , 2009.

[5] Ajit Singh and Upasana Jauhari," A Symmetric Steganography with Secret Sharing and PSNR Analysis for Image Steganography", International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012 2 ISSN 2229-5518.

[6] N.Santoshi, B.Lokeswara Rao, B.Lokeswara Rao, "A Secure and Lossless Adaptive Image Steganography with Mod-4 LSB Replacement Methods Using Image Contrast", International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 1 ISSN 2229-5518.

[7] Kaustubh Choudhary, "Properties of Images in LSB Plane (A Steganalystic Perspective)", International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 1 ISSN 2229-5518.