Extended Fibonacci Series for Selection of Master Pixels Components in Data Hiding

Virendra P Nikam, Sheetal S Dhande
Sipna College of Engineering and Technology
Amravati 444606. India
{virendranikam@gmail.com} {sheetaldhandedandge@gmail.com}

ABSTRACT: *Now a day an information security is a major issue in an IT Sector. An information security becomes complex and more important problem. Much of an organization does their expenditure on securing their data. Achieving security of the local server is not a big issue, but the problem comes When sensitive information transmitted over a wireless network. Encryption/ decryption can be an important tool to help in improving information security. This paper focus on a concept of data hiding process through the use of fabbonacci series that get helps in randomize pixel selection. Randomize approach for pixel selection helps to achieve a good match between original carrier and resultant carrier. we developed techniques for securing data to avoid hacking as well as providing the user with some additional features such as key for integrity and validation of user. In this technique one can secure any type of files by hiding it in carrier media using Fibonacci series. The proposed algorithm is loss-less, key-dependent.*

Keywords: Data Hiding, Fibonacci Series, Master Pixels, Carrier Channels, Wireless Media

DOI: 10.6025/jisr/2020/11/1/1-9

Received: 19 October 2019, Revised 4 December 2019, Accepted 19 December 2019

1. Introduction

The reason for this security and confidentiality is because the underlying communication network over which the transfer of sensitive information is carried out is unreliable and unsecured. Anybody with the proper knowledge and right applications can eavesdrop and learn of the communication and intercept the data transfer which could be very dangerous and even life threatening in some situations. Ideally the internet and the communication network and the routing protocols should exhibit the following the properties:

Security: Security is an important property of the internet. The internet should provide and preserve the confidential and sensitive information that flows through it. The security should be such that only the intended recipient of the information should gain access to it.

Distributed Operation: The internet should be distributed rather than only residing on some centralized server. In the event of the crash the internet should not lose its functionality and continue performing efficiently.

Reliability: Reliable communication is one of the vital properties of the internet. The internet should guarantee the reliable delivery of the information to the intended recipient.

Fault-Tolerance: Fault-tolerance means the ability of the system to operate normally even in the events of failure. Internet should exhibit fault-tolerance so that it keeps on functioning even when there is failure in some part of the internet.

Quality of Service Support: Quality of Service (QoS) is one of the crucial properties in terms of communication. Inter should provide QoS support to various applications and sensitive data and should prioritize them depending on the nature of the data.

Robustness: Internet should be robust in the sense that it should continue functioning normally even in the presence of errors and unexpected situations like invalid input.

All the above mentioned properties are ideal and cannot be practically implemented in the structure and functioning of the internet as it comprises of many networks, different infrastructures: wired, wireless, ad hoc and various mobility models. One such property that cannot be guaranteed in the internet is Security.

Data Hiding is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing messages than cryptography, which only conceals the content of the message not the existence of the message. The original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. In this paper, we will discuss a new concept of selection of pixels for data hiding using fabbonacci series.

This Paper also analysis existing process performance for pixels selection. Wireless transmission of sensitive data should require security from hacker, intruders and many more entities because no one could guarantees of security over wireless media. The primary focus of this paper is to concentrate how efficiently possible to use Fabbonacci series for generation of next pixels in hiding process.

Data hiding embeds messages into digital multimedia Such as image, audio, video etc. through an imperceptible Way. Such technology plays the important role in protecting the privacy, which can be roundly classified as robust watermarking [1] having the ability to resist many attacks, fragile Watermarking [2], [3] being fragile to any modifications, and steganography [4] with the strong undetectability. From the application side, robust watermarking, steganography and fragile watermarking are mainly used for copyright protection, covert communication and integrity authentication respectively. A review of data hiding techniques and a few emerging innovative solutions using data hiding are well introduced in [5].

However, some data hiding techniques destroy the originality of carrier medium that gives an immense clue to intruder about an existence of secret information conceal in it [2]. Some special signals are so precious and cannot be damaged, such as medical imagery, military imagery and law forensics. Therefore, recovering the host signal from the marked signal completely is rather important.

An introduction of Fabbonacci series for selection of Master pixel components for data hiding plays an important role in noise generation in carrier medium. Many of that existing techniques, used either sequential approach or random approach for pixel selection. Whoever each method has its own advantages and disadvantages.

Sequential approach generates noise which is easily predictable and visible for everyone. This is a simple method for pixel selection and it not generating any additional keys during data hiding process. But random approach is complicated and need to keep store pixel numbering through which sequence data hidden in pixels. Randomize approach generates additions keys which receiver requires four Secrete information retrieval.

2. Literature Survey

Kuo et al [16] provide another technique where blocks are divided such that each block has secret information embedded in it. In this reversible technique, a histogram is generated for every block of the image. Embedding space is generated on the basis of computing the minimum and maximum points of the histogram for hiding the secret data which also increase the capacity of the images at the same time.

Naseem et al [17] have proposed the Optimized Bit Plane Splicing technique. This technique is a modification of the traditional bit plane splicing technique where the data is hidden based on the intensity of the pixels. The intensity of each pixel is calculated and arranged into different categories based on their range. Then based on the intensity of a pixel, the required number of bits are selected in a particular plane in which data is hidden. The bits are hidden in a random fashion and the planes are transmitted sporadically therefore improving the efficiency of the algorithm.

2.1. LSB Coding

Analog signals are converted to digital binary sequence by sampling the data with the help of quantization. In order to hide the secret messages using this technique, binary equivalent of the secret message is embedded in the LSB of the binary sequence in the digitized audio file. [18]

2.2. Phase Coding

Phasing coding is one the most effective techniques. In this method, the secret message is embedded in the phase where the reference phase of the hidden data is replaces the phase of the original audio signal. [19]

2.3. Echo Data Hiding

Echo data hiding is an interesting method with hides the secret messages in the form of an echo in the original audio signal. The data is hidden in the parameters of an echo like initial amplitude and decay rate. The signals seem to blend as the offset between them decreases and after a certain point, they are indistinguishable to the human ear. The human ear perceives it as added resonance. This point depends on the quality of the original recording, the type of sound being echoed, and the listener. [20]

2.4. Vacating room before Encryption

For Vacating room before encryption (VRBE), the original images are processed by the data Owner to create vacant room for data embedding before encryption, And the secret data are embedded into the specified positions By the data hider. K. Ma et al. proposed a VRBE based RDH in the encrypted images [3]. For a grayscale image with a size of $M \times N$, it first moves [l / N] rows of pixels that have the least correlation to the top of the image (assume [[l / N] ¡ M)], where l represents the length of message. After that, the LSBs and the original location information of them are embedded into other pixels with a traditional RDH [30], and then the processed image is encrypted and uploaded to the cloud. For a CSP, it can hide and extract data with the first [l / N] rows of pixels. If a user wants to obtain the original image, he can decrypt the image and extract the LSBs and the original location of the top [l / N] rows of pixels, and then recover it. Although it needs extra processing before encryption, it provides an alternative means for RDH in encrypted domain other than VRAE.

2.5. DNA Sequence and Recombinant DNA Technique (DSRDTM)

The proposed DSRDTM consists of a series of hiding steps. Firstly, some secret message is hidden in a fake sequence. Then, the fake sequence and selectable markers are both ligated To a vector DNA plasmid by restriction enzymes and ligase. The plasmid can be further hidden in a bacterial organism, Such as Escherichia coli (E. coli). Finally, the bacterial cells Are concealed with a huge number of dummy cells and be Screened by selective culture.

2.6. Exploiting Modification Direction (EMD)

In 2016, a data hiding scheme based on EMD proposed by Zhang and Wang, the proposed method is used in Neighboring pixels into a group, the purpose is turning into minimal changing for embedding produce. That is, Zhang and Wang design an extraction function as

$$f_e(g_1, g_2, g_3, ..., g_n) = ([\sum_{i=1}^{n} g_t * t]))mod(2n+1)$$

2.7. GEMD (General Exploiting Modification Direction)

The GEMD data hiding method proposed by Kuo and Wang, which changed the weight value and the modulus value to increase hiding capacity, it turns EMD from less than 1bpp upgrades to (n + 1) bpp. GEMD also choose n pixels as one group, GEMD modulus value is changed (2n+1) to, and expand the amount of change that the group pixel can adjust, achieve the balance of payload and image quality. The extraction function as

$$f_e(g_1, g_2, g_3, ..., g_n) = ([\sum_{i=1}^{n} g_t * (2^t - 1)]))mod(2^{n+1})$$

where n is group number, g is the i^{th} pixel value.

2.8. Descrete Wavelet Transform (DWT)

A discrete wavelet transformation approach is made towards audio Steganography to conceal messages. Different properties of waves are varied maintaining minimal deviation of new derived wave from the original wave and also keeping the SNR low such that the original wave and derived are very hard to distinguish under normal condition or by just hearing.

3. Proposed Methodology

Proposed Methodology consist of below steps

3.1. Input Carrier Media

Let the carrieer media as Image which consist of no of pixels. Image have fix dimension *h*w* i.e Height and Width and is a color combination of pixel values consist of three color channels namely called as Red, Green, Blue. Sequence of pixels can be represented as $\{p_1, p_2, p_3, ..., p_n\}$

Figure 1. Carrier Image

let a matrix representation of an carrier image as below So an Carrier image can be represented as

$$I = \int_{i=1}^{width} \int_{j=1}^{height} \{Pij\}$$

If we split pixel *p* into its color componant then pixel *p* = {*r, g, b*}. an individual componant is capable of holding secrete binary bit. However it depend on methodology.

Minimmum capacity of an image *Cmin = r*g*b*nBits* Bits and *Cmax = r*g*b*n*8Bits*

p	*p*	*p*	*p*	*p*	*p*
p	*p*	*p*	*p*	*p*	*p*
p	*p*	*p*	*p*	*p*	*p*
p	*p*	*p*	*p*	*p*	*p*
p	*p*	*p*	*p*	*p*	*p*

Table 1. Pixel Representation of Carrier Image

3.2. Sample Selection by Sequential Approach

Sequential approach is simple and can be demonstrated as, Pixel samples with their position as shown in Table 2.

while hiding data with any approach, pixels are chosen sequentialy from 1, 2, 3,... *n*. Group of noisy pixels are generated sequentially with same sequence position of selecting pixels for data hiding. Visual appearance of carrier image get disturb if large numbers of bits conceals into pixel value. This method is not suitable for real time security applications due to its simplicity.

$$Quantization\ error = Mod\ [Pixel_{result} - Pixel_{original}]$$

is directly proportional to amount of bits conceals in carrier.

Pixel	Postition
$p1$	1
$p2$	2
$p3$	3
$p4$	4
. .	
pn	n

Table 2. Pixels With Positioning

3.3. Sample Selection by Randomize Approach

Randomize approach overcomes drawbacks of sequential sample selection. It is more complicated and generate an additional key to remember where secrete bits are concealed.

As shown in table II, Pixels are chosen randomly $p(x) = Random\ (1, Total_{pixels})$

Additional key generated contains exact numbers of key items as that of no of samples chooen for data concealing.

$$Key = Position\{P_1, P_2, P_3, ..., P_n\}$$

3.4. Sample Selection by Extended Fibonaccii Series

In mathematics, the Fibonacci numbers, commonly denoted fine form a sequence, called the Fibonacci sequence, such that each number is the sum of the two preceding ones, starting from 0 and 1. That is $F_0 = 0\ F_1 = 1$ and $F_n = f_{n-1} + f_{n-2}$.

We are introducing Extended Fibonaccii Series for Sample Pixel Selection.

Algorithm:

```
1) Start
2) Set $Current_{index}$
3) Set $Previous_{index} = Current_{index}$ - 1
4) while ($Current_{index}$ —$Total_{samples}$)
$Previous_{index} = Current_{index}$
$Current_{index} = Current_{index} + Previous_{index}$
if$Current_{index}$— $Totalsample$
$Current_{index} = PreviousCurrent_{index}$
$Previous_{index} = Current_{index} = 1$
end
Select Sample at $Current_{index}$
```

```
end
5) Stop
```

This method avoids the drawback of the randomization approach of generating addition keys during data hiding process. However, it needs to keep remember the only first sample position for data extraction. Let pixels with their positions are represented as

Position	0	1	2	3	4	5	6	7	8	.	.	*n*
Fibonaccii=	0	1	1	2	3	5	8	13	21			*n*

Table 3. Pixels Selection With Fibonacci Series

However problem rises when there are *n* bits for hiding and sample are < *n* . To solve this problem, we set up new start index and do hiding as per fibonacci series.

Position	0	1	2	3	4	5	6	7	8	.	.	*n*
Fibonacci	4	3	7	10	17	27	44	61	105			*n*

Table 4. Extended Fibonacci Series

We continue this process of selection on the new start index until required samples are not selected.

4. Result Analysis

We compare our results with too many existing techniques that introduces noise in carrier media and we found that, extended fibonacci series provides good result. Two signals are compared based on various parameters. Among them Power and Signal to Noise Ratio (PSNR) value are the most important and valuable parameters depending on which two carrier signals are compared.

$$PSNR = 10 * log_{10} (Original_{pixel}/Result_{pixel})$$

and the calculated experimental value of mean square error is

$$MSE = \sum_{i=0}^{n} (Original_{pixel} - Result_{pixel})^2$$

Figure 2. Result by Sequencial Sample Selection

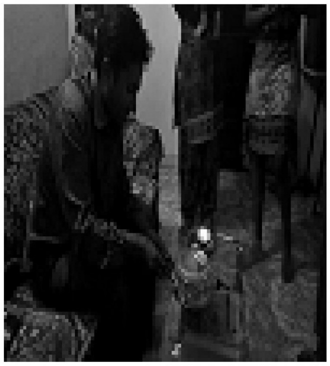

Figure 3. Result by Fibonacci Sample Selection

White rectangle show how noise are introduced sequentialy.

Parameters	Sequential Parameters	Fibonacci Parameters
Mean Square Error	5.34234	1.234
Peak Signal to Noise	80.2342	99.52
Entropy	9830	12548
Mean Intensity	0.43	0.52
Average Mean	0.48	.54
Cross Correlation	0.96	1
Structural Content	0.7	1
Height	100	100
Width	100	100

Table 5. Comparing Fibonacci Series With Sequential Method

Parameters	Random Parameters	Fibonacci Parameters
Mean Square Error	1.53	1.234
Peak Signal to Noise	97.27	99.52
Entropy	1145	12548
Mean Intensity	0.5	0.52
Average Mean	0.53	.54
Cross Correlation	1	1
Structural Content	1	1
Height	100	100
Width	100	100

Table 6. Comparing Fibonacci Series With Random Method

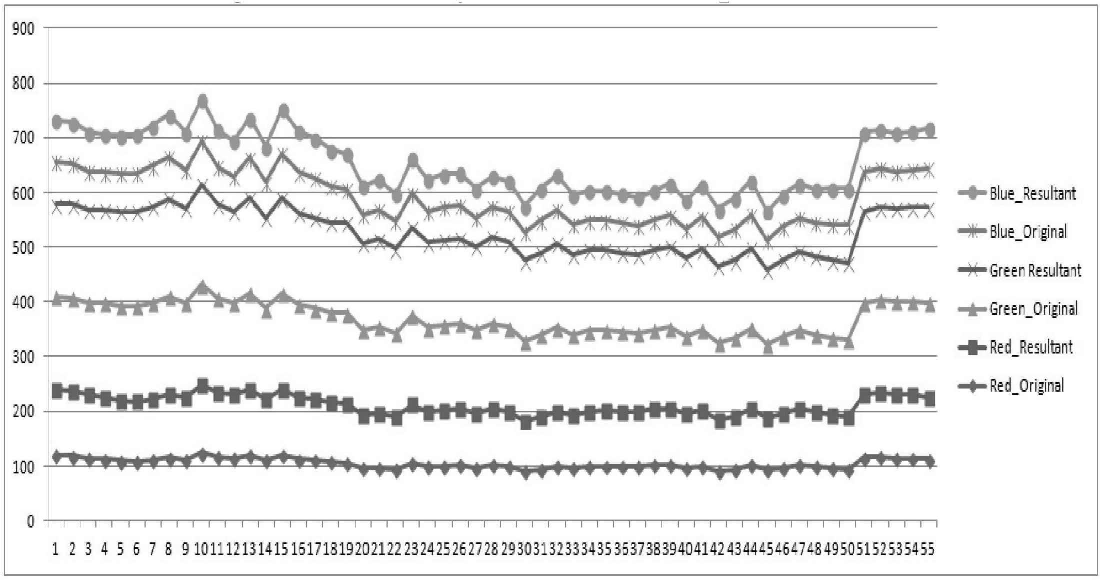

Figure 4. Result by Fibonacci Sample Selection

5. Advantages

Proposed way of Sample Selection by Extended Fibonacci Series have an Advantages

1) No need to keep remember position values of samples where secrete bit data get hidden.

2) Select all image pixel samples.

3) Not too complecated and easy to understand.

4) Probablity of occurance of collision is rare.

6. Conclusion

This work focuses on a new approach of data hiding Using Extended Fibonacci Series. By applying EFS on any carrier channel will help to select samples for data hiding. This sample selection approach helps to reduce noise that created due to sequential sample selection process. Also EFS not require to store any additional key after data hiding process. Comparative study shows that result is far better than available methods for sample selection. This leads to further enhancement of applicability of EFS in security softwares.

References

[1] Ni, Z., Shi, Y. -Q., Ansari, N., Su, W. (2006). Reversible Data Hid-ing, *IEEE Transactions on Circuits and Systems for Video Technology*, 16 (3) 354-362.

[2] Tai, W. -L., Yeh, C. -M., Chang, C. -C. (2009). Reversible data hiding based on histogram modification of pixel differences, *IEEE Transactions on Circuits and Systems for Video Technology*, 19 (6) 906–910.

[3] Zhang, X. (2011). Reversible data hiding in encrypted images, *IEEE Signal Processing Letters*, 18 (4) 255–258.

[4] Hong, W., Chen, T., Wu, H. (2012). An improved reversible data hiding in encrypted images using side match, *IEEE Signal Processing Letters*, 19 (4) 199–202, 2012.

[5] Liao, X., Shu, C. (2015). Reversible data hiding in encrypted im-ages based on absolute mean difference of multiple neighboring pixels, *Journal of Visual Communication and Image Representation*, 28, 21–27.

[6] Qian, Z., Dai, S., Jiang, F., Zhang, X. (2016). Improved joint re-versible data hiding in encrypted images, *Journal of Visual Communication and Image Representation*, 40, p 732-738.

[7] Zhou, J., Sun, W., Dong, L., et al. (2016). Secure reversible image data hiding over encrypted domain via key modulation, *IEEE Transactions on Circuits and Systems for Video Technology*, 26 (3) 441- 452.

[8] Zhang, X. (2012). Separable reversible data hiding in encrypted image, *IEEE Transactions on Information Forensics Security*, 7 (2) 826–832.

[9] Wu, X., Sun, W. (2014). High-capacity reversible data hiding in encrypted images by prediction error, *Signal Processing*, 104, 387-400.

[10] Qian, Z., Zhang, X. (2016). Reversible data hiding in encrypted image with distributed source encoding, *IEEE Transactions on Circuits and Systems for Video Technology*, 26 (4) 636-646.

[11] Qian, Z., Zhang, X., Feng, G. (2016). Reversible data hiding in encrypted images based on progressive recovery, *IEEE Signal Processing Letters*, 23 (11) 1672-1676.

[12] Huang, F., Huang, J., Shi, Y. Q. (2016). New framework for re-versible data hiding in encrypted domain. *IEEE Transactions on Information Forensics and Security*, 11 (12) 2777-2789.

[13] Ma, K., Zhang, W., Zhao, X. (2013). Reversible data hiding in encrypted images by reserving room before encryption, *IEEE Transactions on Information Forensics Security*, 8 (3) 553-562.

[14] Zhang, W., Ma, K., Yu, N. (2014). Reversibility improved data hiding in encrypted images, *Signal Processing*, 94, 118–127, 2014.

[15] Cao, X., Du, L., Wei, X. (2016). High capacity reversible data hiding in encrypted images by patch-level sparse representation, *IEEE Transactions on Cybernetics*, 46 (5) 1132-1143.

[16] Harshvardhan et al. A Survey on Various Data Hiding Techniques and their Comparative Analysis, p.1-9

[17] Naseem, M., Ibrahim M. Hussain., Kamran Khan, M., Aisha Ajmal. (2011). An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding, *International Journal of Computer Applications*, 29 (12), 2011. Foundation of Computer Science, New York, USA, p 36-38.

[18] Nosrati, Masoud., Karimi,Ronak., Hariri, Mehdi. (2011). An introduction to steganography methods, *World Applied Programming*, 1 (3) August 2011. 191-195. WAP journal.

[19] Thampi, Sabu M (2004). Information Hiding Techniques: A Tutorial Review, ISTE-STTP on Network Security and Cryptography, LBSCE 2004, p 1-19.

[20] Bender, W., Gruh, D., Morimoto, N., Lu, A. (1996). Techniques for data Hiding, *IBM SYSTEMS JOURNAL*, 35 (3, 4) 1996, p 313-336.

Author Biographies

Virendra P. Nikam is a PhD Scholar, received his graduation degree from Government college of Engineering, Amravati and post graduation from Rungta college of engineering and technology, Bhilai. His major area of research is data and information security over wireless media.

Dr. Shital S. Dhande is a professor at the department of computer science and engineering having more than 20 years of experience. Her major area of interest is Database, Query Processing and Optimization, Business Intelligence, Web Technologies, etc. She is a also a member of many prestigious bodies like CSI, ISTE, IE- AM, IETE LM etc. She is a recipient of IEEE-ICCCA-2015 Best Paper Award.