Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 22 Issue 2 Version 1.0 Year 2022
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Best Fit Method of Sample Selection in Data Hiding and Extraction

By Virendra P. Nikam & Dr. Shital S. Dhande
SIPNA College of Engineering and Technology

Abstract- Today data security and its transmission over the wireless network need special attention. Intruder always has a watch on sensitive data transmitted over a wireless network. This work proposes an approach that minimizes the quantization error between the original and result carrier by selecting optimize samples during Data Hiding. Propose work find out best matching carrier components during the data hiding process. Results also imply that achieved results are far better than any other steganographic method.

Index Terms: best fit strategy, steganography, quantization error, carrier object, transmission media, data hiding, data extraction etc.

GJCST-E Classification: D.2.11

Strictly as per the compliance and regulations of:

Best Fit Method of Sample Selection in Data Hiding and Extraction

Virendra P. Nikam[α] & Dr. Shital S. Dhande[σ]

Abstract- **Today data security and its transmission over the wireless network need special attention. Intruder always has a watch on sensitive data transmitted over a wireless network. This work proposes an approach that minimizes the quantization error between the original and result carrier by selecting optimize samples during Data Hiding. Propose work find out best matching carrier components during the data hiding process. Results also imply that achieved results are far better than any other steganographic method.**

Index Terms: best fit strategy, steganography, quantization error, carrier object, transmission media, data hiding, data extraction etc.

I. Introduction

Information security is a primary focus for every IT industry. Most of the industries are grown up by analyzing the data that they have. Data is any sort of raw material which can be processed to generate valuable information. Millions of dollars are spent on data security in almost all industries in India and all over the world. In the recent past 10 years, information security is a vital domain that needs special attention in every sector. Raw data is a base pillar of any IT industry. Recent history shows that most of the industries have failed to recover themselves because of not having a proper backup facility. In 2005 India, a major flood in Mumbai itself stops the functioning of more than 2000 small scale IT industries. This implies that the security of information or raw data is very much important. Without security, it's not possible for any IT industry to grow fast and within the expected time.

Now the major issue that comes into focus is how to provide security to sensitive data of an industry? There are many techniques available that are best to provide security to data which is stored either on a separate server system or on a local server system. Many IT Industries prefer to store their data on the server system. Server systems have their own security features and protocols which are enough to protect data. But from the money point of view, it's not convenient to maintain a separate server to stored data especially for those industries which have an annual turnover between 1 to 5 lakh.

The common techniques which are used to provide security to data are cryptography, steganography and watermarking. These three techniques have their own applicability and limitations.

a) Cryptography

Cryptography is an art to convert readable data into an unreadable format. It totally hides the meaning of the original data. Process of converting readable data into unreadable format is called as encryption whereas converting unreadable data into a readable format is called decryption. To perform encryption and decryption, sender and receiver use either the same or different key. Based on the similarity of the key used at sender and receiver side, cryptography is classified as 1. Private key cryptography 2. Public key cryptography. Public key Cryptography uses to separate keys for encryption and decryption. The algorithms like RC2, data Encryption standard, triple Data Encryption standard, advanced encryption standard comes under the category of private key cryptography whereas algorithm likes RSA comes under public-key cryptography.

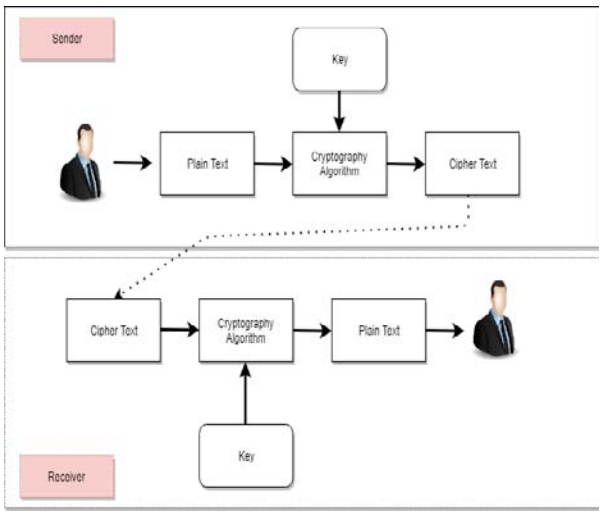

Fig. 1: Overview of Cryptography

Cryptography convert readable data set *fp1; p2; p3; p4; p5:::::; pn g* into unreadable(encrypted) data set *fe1; e2; e3; e4; e5:::::; en g* Cryptography can be defined

Author α: Virendra Nikam is a Ph.D. student who is working on secure data concealing and transmission for wireless networks using steganographic techniques. Data security, information management, and other topics are among his main research interests.
e-mail: virendranikamphd@gmail.com
Author σ: Dr. Shital S. Dhande is a professor at SIPNA College of Engineering and Technology in Amravati, where she teaches computer science and engineering. She's worked in data and information management, security applications, and data query processing for over 20 years. She mentored over ten Ph.D. students and was a member of several important o rganizations such as IEEE, CSI, and others.

as $f(x) = f(p; k)$ for encryption and $f(x) = f(f0(x); k)$ for decryption.

b) Steganography

It's the practice of concealing or hiding hidden information behind a carrier item. With the use of carrier medium, it entirely conceals the existence of data. There is a considerable similarity among Cryptography and steganography that, both hide the real presence of data to an unauthorized user. Result of steganography is exactly similar in appearance with the original carrier object. This is the one mandatory feature of steganography which not allows any change occur in carrier object. Steganography take one carrier object *fc* & secret data *fd* and hide it behind carrier object $f(H) = f(f(c); f(d))$ The similarity of result stego object can be

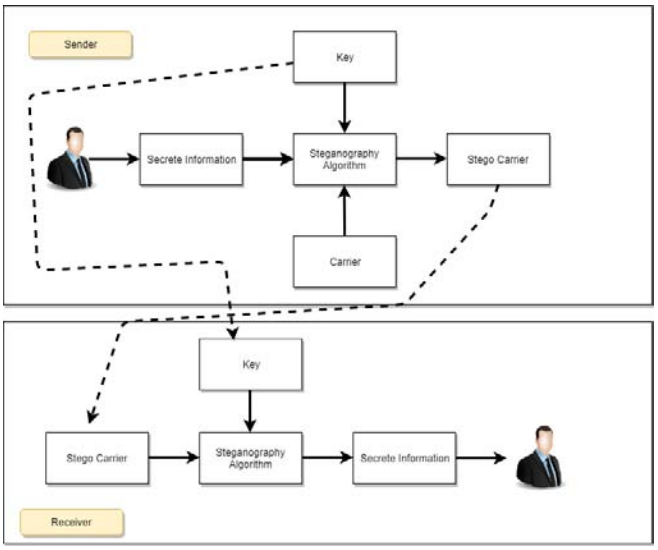

Fig. 2: Overview of Steganography

measured with parameters like peak signal to noise ratio (PSNR), mean square error (MSE), absolute difference, structural content, mean difference, normalized absolute error (NAE) and others. If the result object finds dissimilar visual perceptual quality with original carrier object $f(c)$ $6=$ $f(H)$, the process is not called steganography.

c) Watermarking

It is generally used for copyright protection. Few authors also called watermarking as steganography. Watermarking is of two types 1. Visible watermarking and 2. Invisible watermarking. In watermarking, original carrier replaced with watermark data bits. It's completely changed carrier object especially in visible watermarking. The concept of watermarking was originally designed for copyright protection later on it is expanded for secret data hiding and transmission. This paper focuses on data Hiding and extraction mechanism by optimizing sample selections approach for minimizing quantization error. Quantization error is a difference between result stego object and original carrier object *Qe = jCo -Crj*. Many existing steganography techniques does not focus on minimizing quantization error. Existing technique directly select sample irrespective of its value that results in large quantization error. Maximum quantization error can create difference among original and result carrier object. This paper has a primary focus on effective sample selections with minimum difference.

Basic questions come into mind "How to select optimize sample during Data Hiding process?". This paper proposes an algorithm that finds the best matching carrier sample using best fit strategic approach. The best fit strategic approach is one that generally used in memory allocation. While allocating memory, a primary focus is given on memory fragmentation. Memory gets fragment when memory block of either larger or smaller size get allocated to the required content. Best fit strategic approach reduce memory fragmentation and hence it's a good choice by memory allocator. Best bit strategic approach is chosen by many programmers due to its effective selection of required memory block from available blocks of memory. Consider an item set *fi1; i2; i3; i4; i5:::::; ing* and the required item to search is *fsig* At very first stage, difference among *fsig* and item set please find out *fji1 - sij; ji2 - sij; ji3 - sij; :::jin - sij* An item from item Set with minimum difference *Best match = min jii -sij* Can be chosen as best fit or maximum matched for further processing.

II. Background History

Steganography is the method of concealing hidden information behind a carrier. In its true meaning, steganography is a centuries-old notion that was first executed 300 years ago. People utilized this approach to manually transfer a message from one location to another using a fly in ancient times. The message is coded on the fly's neck after the hair on its back neck is removed. They wait for their neck hair to develop before sending this message to their target. Nowadays, "digital steganography," in which digital data is hidden behind a digital carrier object, is a whole distinct type of steganography. A photo, music, or video might be used as the carrier item. In recent years, many steganography techniques have been invented that make data transfer more secure by preventing an intruder from inferring data.

Least Significant Bit Substitution (LSB) is the original steganography technique, and it includes hiding a secret information bit at the first (from right to left) position of the carrier sample. Let's look at a carrier sample in binary format (0001010*textbf*1) with the secret bit set to 0. After concealing secret bit 0, the output carrier sample is (0001010*textbf*0). This approach is straightforward to use and retains the carrier's audio-

visual perceptual quality. However, because of its simplicity, an attacker may be able to readily find hidden bit locations, thus allowing unlawful data extraction.

By concealing hidden bits at higher and higher LSB places, the problems of the least significant bit replacement approach were eliminated. Moving from the least significant bit (LSB) to the most significant bit (MSB) increases quantization error *Qe*. An intruder can easily detect the existence of secret information bits behind the carrier owing to a discrepancy between the result and the original carrier object caused by a quantization mistake. A quantization error is a number that ranges from 0 to 255.

Spread spectrum analysis, wavelet analysis, and sample selection procedures were offered as ways to reduce quantization error. All of these methods choose the optimal sample carrier and then hide hidden data behind it. These techniques bring quantization error down to an acceptable level. However, each strategy has its own set of benefits and drawbacks. These methods take a long time to implement and are difficult to master. In terms of data concealing capacity, quantization error, time processing, and so on, none of the solutions are perfect.

III. Literature Survey

M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati [1] published a paper in 2011 that described a new approach for detecting hidden information in a 24 bit RGB color picture. After the data has been hidden, carrier samples are connected together to remember where the secret information bits are kept. They're disguising data with a randomized sample selection strategy, which might make the data extraction procedure more complicated and challenging. It connects data samples with each other via a directed data connection list. It also sets aside portion of the carrier sample in order to check for the presence of secret information bits.

Wen-Chung Kuo, Dong-Jin Jiang, and Yu-Chih Huang [2] introduced a data concealing and extraction approach based on block division in 2008. This approach separates the data into numerous blocks, then generates a histogram for each of them. The histogram's lowest and maximum points are found, allowing hidden data to be stored in each block and enhancing its data concealing capability.

Steel hypothetical, audio/video steganography, IP datagram steganography, and other data concealment techniques were introduced by Soumyendu Das, Subhendu Das, Bijoy Bandy opadhyay, and Sugata Sanyal [3] in 2008. The focus is on creating a carrier histogram to determine the amount of space available for data concealing and encryption to increase the security of sensitive data transmitted across an unsecured wireless network.

In 2002, Ming Sun Fu and O.C. Au [4] introduced a halftone picture data-hiding approach. When original multitone photos are unavailable due to force pair toggling, this approach offers a high data concealing capacity. The visual perception of the outcome image's quality is so similar to that of the original carrier that it's impossible to tell them apart.

H. B. Kekre, Archana Athawale, Archana Athawale, Archana Athawale, and Uttara Athawale [6] suggested a Data Concealing technique for hiding data in audio by producing stego audio carriers in 2010. This recommends that instead than hiding data directly in the LSB of an audio sample, the parity of the sample should be calculated first, and then the choice to hide secret sample information be made. An intruder will find it incredibly difficult to estimate where secret information bits are concealed in a carrier using this method.

Data Hiding utilizing video as a carrier was proposed by Xiaoyin Qi, Xiaoni Li, Mianshu Chen, and Hexin Chen [7] in 2011. This method use an add-up strategy to choose the best sample from a carrier that conceals hidden information. In this approach, a 4X4 DCT block is scanned in a zigzag pattern to obtain the best matching sample.

By breaking a picture into numerous blocks, T. Hong, W. Chen, and H. Wu [8] describe a Data Hiding technique in 2012. Finding the smoothness of a carrier sample is used to extract data. The data extraction technique does not include the four edges of each block. When the size of a block is smaller, the extraction process slows down. On the receiver side, the extraction process is completed by measuring the perceptible smoothness to at least one.

In 2013, C. Qin, C.-C. Chang, Y.-H. Huang, and L.-T. Liao introduced a prediction-based reversible data concealment strategy that chooses image carrier samples based on their distribution features. To create a predicted picture with similar structural content to the original carrier image, an image in-painting approach is applied. To incorporate hidden information bits, the histogram of the difference is altered. Secret information bits can be retrieved precisely and without alteration on the receiver side. The prediction technique is used to estimate the covered picture pixels and quantization error before moving on to Data Hiding.

In 2014, X. Zhang, Z. Qian, G. Feng, and Y. Ren [10] suggested using lossless compression to hide data in encrypted photos. The encrypted image's route is compressed with LDPC coding before being implanted with extra secret info. Encrypted data has a high level of quality. Hidden data is successfully retrieved on the receiver side. LDPC coding is used to hide data at the 4*th* LSB of an image.

In 2015, Jiantao Zhou, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang suggested a datahiding technique in the encrypted domain [11]. There is no need to disclose a private

encryption key because images are encrypted and decrypted with a public key. This method encrypts sensitive information using public-key cryptography once it is hidden in a carrier. This method eliminates the need for additional transmission expenses to send secret encryption techniques. The picture is decrypted with a separate key on the receiver's end, and then the concealed bits are retrieved.

IV. Proposed Methodology

Proposed methodology concerned with an actual implementation of suggested work. It includes a data flow diagram, algorithms, system model, etc. Searching and locating an optimize sample is not a simple task. It needs lots of comparison and sorting of intermediate results. The overall process is divided into a total four states

a) Carrier Selection.
b) Carrier Classification.
c) Searching Best Fit Sample from Class.
d) Updating Result Carrier with Newly Find Best-Fit Sample.

a) Carrier Selection

A carrier is an object that has the capability to carry sensitive data. In the proposed concept, carrier may be an image, audio or video. Carrier is an integration of samples *cr* = R*in*=1 *fcig* Which can be consist of 8 bits only. If a carrier is an image, it consists of RGB colour combination and represented each colour (RGB) with 8 bits. If a carrier is an audio, it consists of left and right stereo channels. Each carrier sample *ci* have a minimum value 0 and maximum value 255. For an image carrier sample *ci* is an integration of RGB values R (*R; G; B*) . While processing image as a carrier, colour channels are considered and manipulated separately.

b) Carrier Classification

Carriers are classified based on hiding position of the sensitive information bit. If sensitive information is decided to hide at 3*rd* position of carrier binary, then samples are classified accordingly. An effectiveness of proposed algorithm entirely depends on hiding the position of the secret information bit. Security is a major issue that is achieved with high complexity. Security level gets increase from the Least Significant Bit (LSB) to Most Significant Bit (MSB).The number of item in each class gets affected by the position of secret information bit. It is always better to classify carrier samples as per the MSB position. Security of data can be increased with higher MSB position. However, all samples of carrier are not sure in table 1 due to its large size. Samples are equally divided that is 128 in class 0 and class 1 each.

Table I: Carrier Samples Classification

Class 0	Binary	Class 1	Binary
0	00000000	4	00000100
1	00000001	5	00000101
2	00000010	6	00000110
3	00000011	7	00000111
8	00001000	12	00001100
9	00001001	13	00001101
10	00001010	14	00001110
11	00001011	15	00001111
16	00010000	20	00010100
17	00010001	21	00010101
18	00010010	22	00010110
19	00010011	23	00010111

c) Searching Best Fit Sample from Class

The best fit sample searches according to the secret information bit. If secret information bit is 0, best fit sample search into Class 0 else it is searched in class 1. The best fit sample is a sample with a minimum difference with the original sample. Suppose secret bit is 0 and sample taken for hiding it is equal to (7)10 = (00000111)2. At position 3, bit 1 is present. After replacing 3*rd* bit with 0, the final value of the sample becomes (00000011)2 = (3)10. In this case, Quantization error *Qe* = *j*3 - 7*j* = 4 . Propose approach help to focus on minimizing this condition error. Find out the best-fitted sample in class 0 which is sample (8)10 = (00001000)2. After finding best sample, Quantization error becomes *Qe* = *j*8 - 1*j* = 1.

d) Updating Result Carrier with Newly Find Best-Fit Sample

While doing replacement of original carrier sample with resultant sample, a proposed algorithm takes care for not generating quantization error more than ±16. Effectiveness of any steganography algorithm depends on the difference between result and original carrier object. The audiovisual perceptual quality of carrier gets affected with large quantization value which may violate a definition of steganography. Result sample after setting it to carrier will change its originality which is measured by parameters like peak signal to noise ratio, mean square error, absolute difference, minimum difference, structural content, cross correlation etc.

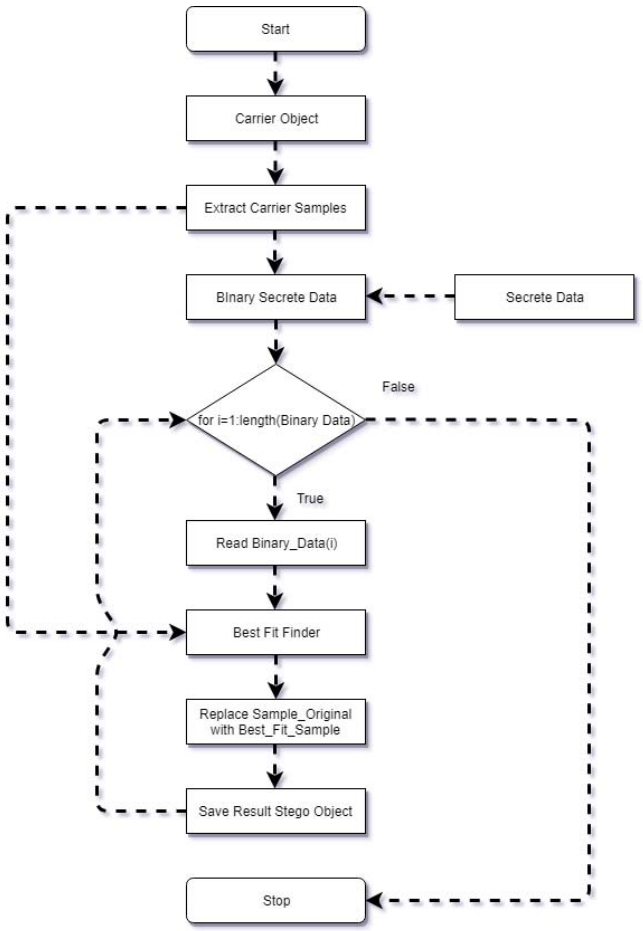

Fig. 3: Data Flow Diagram

As shown in the data flow diagram, user first select carrier object which may be anything like a picture, audio or video. Samples are extracted from this carrier which is given to best fit finder. Sensitive information given by the user is converted into its equivalent binary format. For each bit of binary sensitive information, best fit finder locates best carrier samples with minimum quantization error *Qe*. Loop continues its execution until all binary bits of secret pieces of information get completely hidden behind carrier samples. Below algorithm is used for Data Hiding process which is effectively implemented and executed by proposed system. Effectiveness of Data Hiding algorithm is based on at what position secret information bit get hidden?. The algorithm does not focus on the position of secret bits in the carrier object. It is the generalized algorithm which can be fit for any carrier with any position.

Propose concept deal with information hiding in a carrier by minimizing its quantization error so that the difference between resultant and original carrier should be minimum as possible as.

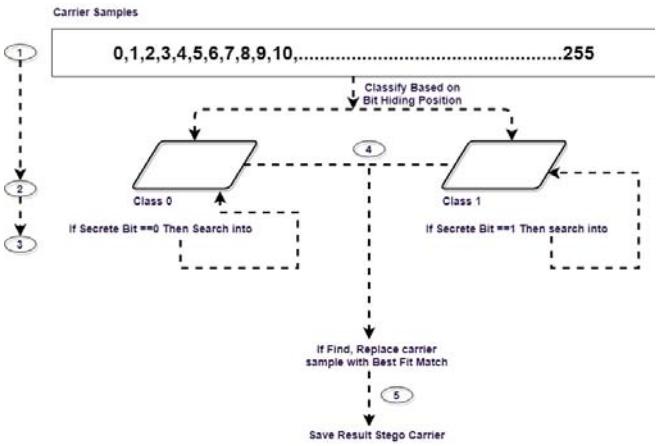

Fig. 4: Detailed Process Data Flow Diagram

Figure 4 demonstrates the proposed Data Hiding approach with detailed process data flow diagram. Carrier samples consist of 8 bits which have minimum value 0 and maximum value 255. These samples classified into class 0 and class 1 based on at what position secret information bit get it done? Suppose sender decides to hide secret information bit at third position, class 0 contains all the values which have 0 value at their third position of binary and class 1 contain all sample having 1 at 3rd position. If secret information bit equal to 0, optimized samples will be searched in Class 0 else search into class 1.

Algorithm

1 Start
2 Input Carrier c_r
3 Extract Carrier Sample c_s
4 Input secrete information s_i
5 Convert s_i to Binary B_{s_i}
6 For i 1 to count(B_{s_i})
  Find Best Fit Sample c_s' from c_s
  c_s c_s'
  c_r c_s
  End
7 Save c_r
8 Stop

Let's illustrate the algorithm with a specified example. Consider a set of carrier samples 10; 24; 30;

50:::::*n* and secret binary information 00101100. Read the first bit of secret binary information from Most Significant Bit to Least Significant Bit. The first bit is 0 and supposes carrier sample is (23)10 = (00010111)2 . An algorithm decided to hide secret information bit at 3*rd* position from LSB side. An algorithm finds the best matching carrier sample from a set of carrier samples i.e (24)10 = (00011000)2 With selected best fit sample, contribution error *Qe* = *j*23 - 24*j* = 1.

V. Result Analysis

Result analysis is used to compare the proposed concept output with existing results. An outcome of result analysis must be the final decision that it shows its applicability, acceptability and it's implications.

Fig. 5: 1, 2

From figure 5, 1 represent to original image whereas 2 represents result carrier image. From above images, one can conclude that propose best fit sample selection strategy for Data Hiding preserve the visual perceptual quality of carrier. The similarity between these two images can be measured with the other parameters shown in below Table II and Table III. Propose concept have been tested on more than 50 carrier images of uncompressed types. We intentionally proceed with uncompressed carrier to successfully extract hidden data.

Propose concept compared with existing methods like least significant bit substitution (LSB), higher LSB and many more. From Table II, quantization error occurs is very from 0 to 8. It implies that, propose a steganographic technique generates very less noise/ quantization error which best suited for an image as a carrier. For audio, quantization error *Qe* is tolerable up to ±16 . Hence it is also fit for audio-based steganography. Parameters mentioned in table II are used to compare the original and resultant carrier object. From table II, it is concluded that with the proposed best fit strategy, it is possible to maintain too much similarity between original and result carrier. Structural content, cross-correlation and normalized absolute error(NAE) remain untouched which indicates its effectiveness and acceptability of the proposed algorithm.

Table II: Parameter Comparison

Average Red	Average Green	Average Blue	MSE	PSNR	Max Diff	Min Diff	Average Diff	NAE	Cross Correlation	Structural Content
0.39	0.27	0.37	2.72	43.79	71	0	0.34	0	1	1
0.36	0.25	0.32	1.21	12.52	25	0	0.21	0	1	1
0.34	0.21	0.29	1.89	10.58	10	0	0.25	0	1	1
0.41	0.22	0.40	0.52	13.56	14	0	0.26	0	1	1

means square error (MSE) = *n*1 P*n i*=1 (*ci - c0 i*)2, peak signal to noise ratio = 10 ∗ log10 *MAX MSE*2 , Min difference = *Min jco - crj* , Max difference = *Max jco – crj*, nor *n i*=1 P*m j*=1*i*=1correlation (CC) = (*f* ∗ *g*) (*τ*) Δ *1 f* ¯(*t*)*g* (*T* + *τ*) *dt* and structural content P*n i*=1 P*m j*=1(*coij*)2 P*n i*=1 P*m j*=1(*crij*)2 is a measure of the difference between original and result carrier. Table II imply that difference occurs at a minimum level.

Table III: Parameter Comparison Result Analysis

Image Type	Red Mean	Green Mean	Blue Mean	Mean	Pure Height	Pure Width	Entropy
Original Image	105	108	81	221598	50	45	449.33
Result Image	104	108	81	221395	50	45	449.33

Entropy is a measure of information represented by the carrier object. Samples which are closer to 0 and 255 does not contributes to entropy. From table III, one can conclude that with proposing a best-fit strategic approach for sample selections of carrier will reduce the quantization error at minimum level. Changes occur in the image as a carrier shown with the parameters like average red $Avg_{red} = (\sum_{ri=1}^{n} P_{ri})/n$, average green $Avg_{green} = (\sum_{gi=1}^{n} P_{gi})/n$, , average blue $Avg_{blue} = \sum_{bi=1}^{n} P_{bi})/n$ and $Entropy = \sum kP_k \log_2(P_k)$ etc.

Table IV: Difference Between Original and Result Carrier Sample

Red Original	Red Result	*Qe*	Secrete Bit	Green Original	Green Result	*Qe*	Secrete Bit	Blue Original	Blue Result	*Qe*	Secrete Bit
34	34	0	0	25	23	2	0	16	15	1	1
51	51	0	0	42	39	3	0	35	35	0	0
48	48	0	0	40	40	0	1	37	40	3	1
166	166	0	0	127	128	1	0	132	132	0	0
181	181	0	0	138	138	0	1	147	143	4	1
155	151	4	0	113	111	2	1	127	127	0	1
173	176	3	0	140	140	0	1	157	160	3	0
119	119	0	0	115	115	0	0	138	135	3	0
187	183	4	0	167	167	0	0	192	192	0	0
200	199	1	0	172	172	0	1	197	200	3	1
108	112	4	0	93	93	0	1	112	112	0	0
26	23	3	0	20	24	4	1	24	23	1	0
20	20	0	0	14	14	0	1	16	15	1	1
255	247	8	0	210	207	3	1	220	220	0	1
227	227	0	0	176	175	1	1	191	191	0	1
212	212	0	0	174	174	0	1	197	200	3	1
68	68	0	0	59	59	0	1	90	87	3	0
161	161	0	0	140	144	4	0	173	173	0	1
221	224	3	0	185	185	0	1	221	224	3	0
194	194	0	0	158	158	0	1	194	194	0	0
146	146	0	0	123	119	4	0	151	151	0	0
113	113	0	0	103	103	0	0	114	114	0	0
101	101	0	0	94	96	2	0	102	104	2	1
87	87	0	0	80	80	0	0	87	87	0	0
74	71	3	0	57	57	0	1	37	37	0	0
55	55	0	0	36	36	0	0	22	22	0	0
71	71	0	0	47	48	1	0	45	45	0	1

VI. Conclusion

Table II, III, IV shows that quantization error occurs with the proposed approach is at its minimum level. This concept also preserves the audiovisual perceptual quality of carrier due to which it will be a future choice by many security application developers for transmitting sensitive data over insecure wireless network. The best fit strategic approach is applicable to all types of carrier media including an image, audio, and video. It does not affect size, length at other parameters of carrier.

VII. Future Scope

Future scope concentrates on limitation of proposed work. Even the proposed system reduces quantization error at the minimum level, searching for the best fit sample is time-consuming and needs to have a precise and accurate approach. The number of iterations required to find out the best fit sample is directly proportional to number of samples present in carrier. If propose work requires to avoid searching iterations for the same samples which reduce its overall implementation time.

References Références Referencias

1. M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati, Embedding stegotext in cover images using linked list concepts and LSB technique, Journal of American Science, Vol. 7, No. 6, 2011, pp. 97-100.
2. Wen-Chung Kuo, Dong-Jin Jiang, Yu-Chih Huang, A Reversible Data Hiding Scheme Based on Block Division, Congress on Image and Signal Processing, Vol. 1, 27-30 May 2008, pp. 365-369
3. Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal, Steganography and Steganalysis: Different Approaches, International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008, Serial Publications, pp. 1-11.
4. Ming Sun Fu and O.C. Au, Data hiding watermarking for halftone images", IEEE

Transactions on Image Processing, Vol.11, No. 4, Apr. 2002, pp.477-484.

5. Sandipan Dey, Ajith Abraham, Sugata Sanyal, An LSB Data Hiding Technique Using Prime Numbers, IEEE Third International Symposium on Information Assurance and Security, Manchester, United Kingdom, IEEE Computer Society press, USA, 29 31 Aug. 2007, pp.101-106.
6. H. B. Kekre, Archana Athawale, Archana Athawale, Uttara Athawale, Information Hiding in Audio Signals, International Journal of Computer Applications IJCA, Vol. 7, No. 9, Foundation of Computer Science, New York, USA, pp. 14-19 2010.
7. Xiaoyin Qi, Xiaoni Li, Mianshu Chen, Hexin Chen, Research on CAVLC audiovideo synchronization coding approach based on H.264, IEEE International Conference on Uncertainty Reasoning and Knowledge Engineering (URKE), Vol. 2, 4- 7 Aug. 2011, pp.123-126.
8. T. Hong, W. Chen and H. Wu, An improved reversible data hiding in encrypted images using side match, IEEE Signal Processing Lett., vol.19, no. 4, pp. 199-202, 2012.
9. C. Qin, C. -C. Chang, Y.-H. Huang, and L.-T. Liao, An in painting Assisted reversible steganographic scheme using a histogram shifting mechanism, IEEE Trans. Circuits Syst . Video Technol., vol. 23, no. 7, pp. 1109-1118, 2013.
10. X. Zhang, Z. Qian, G. Feng, and Y. Ren,Efficient reversible data hiding in encrypted images, J. Vis. Commun. Image R., vol. 25, no. 2, pp. 322- 328, 2014.
11. Jiantao Zhou, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au Yuan Yan Tang,Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation, IEEE Trans. On Circuits and Systems for Video Technology, vol. 26, issue 3, pp.441 452,2015.
12. Po-Chun Chang, Kuo-Liang Chung, Jiann-Jone Chen, Chien-Hsiung Lin ,etc. A DCT/DST-based error propagation-free data hiding algorithm for HEVC intracoded frames [J]. Journal of Visual Communication & Image Representation. 2013, 25(2):239253
13. A Piva, R Caldelli, F Filippini. Data hiding for error concealment in H.264/AVC[C]. IEEE Workshop on Multimedia Signal Processing, 2004:199-202
14. Lin T, Lie W, Tsai D, Lin G. Error Resilient Coding Based on Reversible Data Embedding Technique for H. 264/AVC Video[C]. IEEE International Confer ence on Multimedia and Expo, (2005) :1174-1177
15. SD Lin, HC Meng, YL Su. A novel error resilience using reversible data embedding in H.264/AVC[C]. International Conference on Information, 2008, 7(5):1-5
16. X. J. Ma, Z. T. Li, J. L and W. D. Wang. Data Hiding in H.264/AVC Streams with Limited Intra-Frame Distortion Drift [C]. Computer network and Multi media Technology, CNMT 2009.
17. X. J. Ma, Z. T. Li, H. Tu, B. Zhang. A data hiding algorithm for H. 264/AVC video streams without Intra frame Distortion Drift [J]. IEEE Trans. Circuits Syst. Video Technol. 2010, 20(10):13201330.
18. Y.X. Liu, M.S. Hu, X.J. Ma, H.G. Zhao. A new robust data hiding method for H.264/AVC without intra-frame distortion drift [J]. Neu rocomputing. 201 5,1076-1085