

# Credi-Crypt: An Unpremeditated Anti-Counterfeiting Method For Credit Card Transaction System

M.Tech. Scholar Shaik Fouziya Asst. Prof. Mr. A.M. Shafeeulla Asst. Prof. Mr. D. Dhana Sekhar

Department of Electronics & Communication Engineering  
MJR College of Engineering & Technology, Piler, AP, India.

**Abstract** - Data encryption is essential for e-commerce. Here we propose a method for covering sensible credit card data in a random backdrop picture externally the sensible data going presented in unrestricted areas. This paper also proposed to merge the Cryptographic and Steganography technique to implement a good protection solution for credit card transactions. The advanced method appropriates a cryptographic cipher and Arithmetic Coding method to protect data inside a covered picture and later transfer it to the target across the web network. This paper also presents an extra cover for improved protection through the use of the Hamming Code. A complete examination is done to differentiate our method among other famous techniques like DCT and DWT.

**Keywords**- Cryptography, Arithmetic Coding, Bit Plane Substitution, Hamming Code, DWT, Digital Image Watermarking.

## I. INTRODUCTION

Including a part of Cryptography, the art, and science of composing protected communications in such a process that no individual separate from that sender and indicated receiver, assumes the continuation of the communication, a kind of protection for uncertainty is described as Steganography. During digital Steganography, electronic communications may include steganographic coding inside of a transport layer, such as a text file, picture file, application or rules. Media files are absolute to steganographic transmission because of their huge volume.

One of the digital Steganographic methods includes covering communications in the lowest portions of pictures or media files. The robustness of the encryption depends upon the method applied to encode this steganodata. The main purpose of creating Steganographic encoding hard to identify is to assure that certain modifications to that cover picture with the injection of the inserted image is negligible. DFT, Wavelet converts, however our innovation does lossless code [3] for covering data (credit card information) as a watermark. We use arithmetic coding along with cryptography to encrypt the entire credit card data and then embed it onto the picture. Arithmetic coding unlike variable-length codes generates non-block codes.

In arithmetic coding [3], a one to one correspondence between source symbols and code words does not exist. An entire sequence of source symbols (or message) is assigned a single arithmetic code word. The code itself defines the interval of real numbers between 0 and 1. Since the number of symbols in the information

improvements, the interval used to represent it becomes smaller and the number of message units (say, bits)

needed to describe the period grows long, thus presenting this more secure to transfer data. Every symbol of this information decreases the size of the period by its probability of occurrence. When all is said in done, each progression of the encoding procedure, aside from the absolute last, is the equivalent. The encoder has fundamentally only three bits of information to consider: the following image that should be encoded, the present interim (at the very beginning of the encoding procedure, the interim is set to  $[0, 1]$ ), yet that will change) and the probabilities the model allows to every one of the different images.

The encoder partitions the present interim into sub-interims, each speaking to a small amount of the present interim corresponding to the likelihood of that image in the present setting. Whichever interim relates to the genuine image that is alongside be encoded turns into the interim utilized in the subsequent stage. The last subinterval gives the number-crunching code for the info information arrangement.

## II. EXISTING SYSTEM

While present day steganography is developing progressively differing, steganography is in a general sense dependent on issues that are hard to comprehend. An issue might be troublesome in light of the fact that its answer requires some mystery information, for example, unscrambling a scrambled message or marking some computerized report. The issue may likewise be hard in light of the fact that it is characteristically hard to finish, for example, finding a message that creates a given hash

esteem. The field of cryptography to steganography is incorporated, holds onto different uses too. With only a couple of fundamental cryptographic instruments, it is conceivable to manufacture expand plans and conventions that enable us to pay utilizing electronic cash [4]. Here we have utilized one cryptographic instrument to fabricate a less ground-breaking and dependable convention to conceal the Master card data from the interloper.

### III. PROPOSED SYSTEM

To defeat the current issue, Hamming codes [5] are blunder identification rectification codes, identifying two synchronous piece mistakes, and redressing single piece blunders. Scientifically, they are direct square codes. Albeit principally utilized in correspondence, Hamming codes additionally effectively introduce Data Redundancy, broadening their utilization into Steganography. Somewhat plane of a picture is a lot of bits having a similar situation in the separate parallel number.

For instance, for 16-piece information portrayal, there are 16 piece planes: the main piece plane contains the arrangement of the most noteworthy piece and the sixteenth contains the least huge piece. The most huge piece plane gives the harshest yet the most basic estimation of estimations of a medium, and the lesser the quantity of the bit plane, the less is its commitment to the last stage. In bit plane substitution we substitute least noteworthy bits with our ideal information since these LSB's are viewed as outwardly repetitive, it doesn't debase the picture.

### IV. METHODOLOGY

The examinations are executed in MATLAB 2016b running on Windows stage and Linux stage.

#### 1. At Encoding Site (Customer Name):

We have expected that, as a rule, the length of a name on any charge card is restricted to a limit of 20 letters in order (counting spaces). The client is provoked for the entering the name on the card (allude Figure 1). The encryption method consolidated here is the transformation of charge card data (unequivocally the client name on the card) to double frame.

The calculation utilized depends on the in order position of the letter sets in the string entered as client name. Start to finish has been numbered from 1 to 26 of alphabets. So a letters in order in the client name will relate to its sequential situation, in the code. The got number or position is changed over to the 6 digit paired structure, in order to keep entire stream of bits constantly a

significantly number which will make greater vagueness for interloper. The procedure is iterative until entire string is checked.

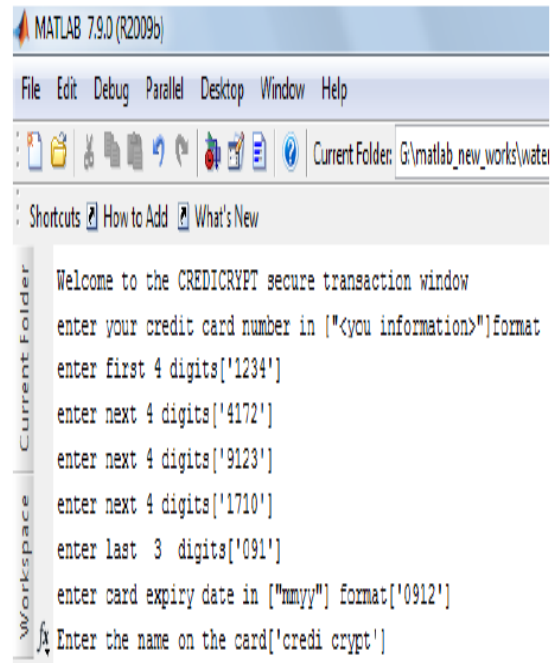


Figure 1. The input data user interface.

This will frame our figure content. The intangibility is additionally improved by acquainting excess with the figure message through Hamming code [8]. A hamming code word was created for each character in the 'Client Name' string. As referenced already, each character was encoded as a 6 piece paired word. Utilizing the equation,

$$2^r \geq m + r + 1 \quad (1)$$

Where r is the number of repetitive bits, m is the length of information, the quantity of excess bits for the 6 piece figure content is discovered to be 10 bits. Henceforth utilizing a (10, 4) Hamming generator lattice, hamming codes for every one of the characters were created. Subsequently, now each character is a 10 piece information word. Therefore, the all-out figure content length was currently 10\* (length of name), making it constantly factor, further muddling the distinguish capacity of the shrouded information.

The length of the string was likewise changed over into a (11, 4) hamming code before inserting it into the spread picture. Thus now the information to be inserted onto the spread picture is the 'Client Name' string with each characters now a 10 piece information word and the length of the string which was an 11-bit information word.

## 2. At Encoding Site (For Customer Card Number):

For encryption of the charge card number we have accepted a Visa number has a 16 digit novel number notwithstanding the huge 3 digit CVV number which is vital for every single online exchange. The calculation likewise encodes the expiry date in (mm-yy position 4 digits), which is crucial for web exchanges. We take these 19+4 digits independently as  $4+4+4+4+3+4$  squares of information and encode them independently [9]. The client inputs the numbers in a consecutive way as provoked by the program in the arrangement as appeared in the Figure 1. The image set for this trial is (0-9) and the comparing image probabilities are as found from enormous information test space. The number juggling encoder takes these probabilities and the image set just as the information succession and yields the lower scope of the last subinterval.

A case of number juggling coding is appeared underneath in Figure 2. After the number-crunching coding process like the above demonstrated model we acquire six twofold exactness esteems relating to the six info arrangements. We round these to six noteworthy digits and afterward convert it to paired utilizing our encoding calculation. Table 1 delineates the aftereffects of the encoded method for an example input. This code word, alongside the figure content acquired in (A) would now be able to be installed into the 'LENA' picture (refer Figure.3) and the picture is packed and afterward sent to the receiver.

Source Symbol	Probability	Initial Subinterval
$a_1$	0.2	[0.0, 0.2)
$a_2$	0.2	[0.2, 0.4)
$a_3$	0.4	[0.4, 0.8)
$a_4$	0.2	[0.8, 1.0)

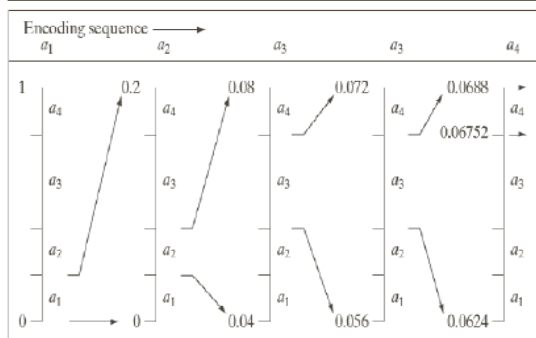


Figure 2. An example of arithmetic coding [18].

Along these lines the whole charge card data has been implanted in the pixels of the picture (refer Figure 4). Different degree of security level has been coordinated and applied on the client data so as to keep up security administrations like information secrecy and information trustworthiness. Along these lines a three level security conspire is given.

TABLE 1. STEPS TO ENCODE A CREDIT CARD NUMBER

Input data sequence	1234
Corresponding code word	0.161389592813131
Code word in six significant digit	161390
Equivalent 20-bit binary	00100111011001101110



Figure 3. An original LENA image used for embedding data (1024\*1024).



Figure 4. The Embedded Image (1024\*1024).

## 3. At Decoding Site (Customer Name):

In the wake of getting the implanted picture, the recipient will do the unscrambling procedure utilizing translating programming which utilizes the definite invert process. Right off the bat, the length of the 'Client name' string is recouped. On the basis of that, remaining data bits are recovered from the image following the reverse algorithm.

Next, the excess bits are expelled with the assistance of a similar hamming code lattice. The removed code word will be conveyed to the decoder. The decoder will continue removing 6 adjoining bits from the got steam of bits (which will be several of 6 consistently) and convert it to decimal structure whose range will be 1 to 26. At that point decimal information will be mapped to the situation of letter set and relating letter set will be remembered for the yield string. This recursive procedure will get the first

client data (the printed name) to the collector. The decoder presently continues to decipher the card number.

#### 4. At The Decoding Side/Receiver Side (For Customer Card Number):

The recipient must have our disentangling calculation. Notwithstanding these the image likelihood, image set and the length of the grouping must be known. On the off chance that a secret phrase was set at the encoding end, at that point the client must enter the equivalent here. The bits are acquired utilizing our switch calculation. Table II: illustrates the decoding procedure for the input data in Table 1.

TABLE 2. STEPS TO DECODE A CREDIT CARD NUMBER

Binary data from image after concatenation	00100111011001101110
Corresponding decimal number	161390
Decimal number after division by $10^6$	0.161390
Obtained credit card number	1234

## V. CONCLUSION

We have fundamentally conceptualized and executed a dependable framework which will revolutionize the manner in which delicate information are being moved by means of web. We have had the option to accomplish every one of our destinations which were set for this framework and furthermore defeat difficulties presented in the manner effectively. The idea which we have created is tried utilizing MATLAB 2016B. We have contrasted our system and other revealed strategies and the outcomes show a huge improvement in intangibility and strength over different methods.

The method is cheap and can be effectively utilized inside a gathering of frameworks. Here we have additionally attempted to contrast our lossless procedure and the lossy watermarking strategies like DWT, DCT to show that this system can be successfully utilized in future uses of charge card data security. Likewise taking a gander at a greater picture, it very well may be utilized as a procedure which can be utilized to counter unapproved access of touchy data over the web. Therefore we accept that this paper in its own particular manner will make a noteworthy commitment in the field of web based business.

The utilization of this framework is huge and not restricted to online business. In any case, we have begun its utilization utilizing charge card data. While investigating different applications numerous difficulties may emerge be that as it may, removing a leaf from the well known expression "Technology continuously requests for invention. The person always requests for

innovation. When both these factors try to satisfy each other the result is always originality".

## REFERENCES

- [1]. Ali Al-Haj "Combined DWT-DCT Digital Image Watermarking". Journal of Computer Science 3(9): 740- 746, 2007.
- [2]. ShikhaTripathi, R.C. Jain et al, "Novel DCT and DWT based Watermarking Techniques for Digital Images". 18<sup>th</sup> International Conference on Pattern Recognition.
- [3]. Ian H Witten, Radford M Neal, John G Clemens "Arithmetic Coding for Data Compression".
- [4]. Hegde, C.; Manu, S.; Shenoy, P.D.; Venugopal, K.R.; Patnaik, L.M. "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications", Advanced Computing and Communications, 2008. ADCOM 2008. 16th International Conference on; Publication Year: 2008 , Page(s): 65 – 72
- [5]. [Chin-Chen Chang; The DucKieu; Yung-Chen Chou; "A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images", Electronic Commerce and Security, 2008 International Symposium on., Publication Year: 2008 , Page(s): 16 – 21
- [6]. Hang Min – Sun, King Hang Wang, Chih- Chang Liang, YihSein Kao, "A LSB Compatible Steganography".
- [7]. Chan, C. and L. Cheng, 2004. Hiding Data in Images by simple LSB substitution, Pattern Recognition, 37(3):469 – 474.
- [8]. Zhao-Xia Yin; Chin-Chen Chang; Yan-Ping Zhang; "A High Embedding Efficiency Steganography Scheme for Wet Paper Codes" Information Assurance and Security, 2009. IAS '09. Fifth International Conference on Volume: 2 Publication Year: 2009 , Page(s): 611 - 614
- [9]. Ravishankar, S; Hariharan, Santosh and Kumar, Naveen V.; 'A Reliable Anti- counterfeiting technique using Lossless Code', Proc. Of The 2010 International conference on Image Processing, Computer Vision and Pattern Recognition (IPCV '10).

### Author's Profile

**Shaik Fouziya** Pursuing M.Tech at MJR College of Engineering & Technology, Department of ECE, Piler, Chittoor Dist.

**A.M. Shafeeulla** Working as a Assistant Professor in MJR College of engineering & technology, Department of ECE, Piler, Chittoor Dist.

**D. Dhana Sekhar** Working as a Assistant Professor in MJR College of Engineering & Technology, Department of ECE, Piler, Chittoor Dist.