IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 11, November 2015.
www.ijiset.com
ISSN 2348 – 7968

An innovative loom for secure diffusion of Images

Murali Majji[1], U.V Chandra Sekhar [2]

1 Computer Science and Engineering, Raghu Engineering College, Visakhapatnam, Andhra Pradesh, India

2 Computer Science and Engineering, Raghu Engineering College, Visakhapatnam, Andhra Pradesh, India

Abstract

The abstract should summarize the content of this paper. In this paper, an innovative loom is designed for diffusing images securely using a technique called Godelization**.** The image which is to be transmitted is transformed into a sequence called Gödel Number Sequence (GNS) using a new technique called Godelization. This is compressed using Alphabetic coding (AC) and encrypted by an encryption method. This encryption string is transmitted and reconstructed at the decoding end by using the reverse process. The key which is to be transmitted is transformed into a sequence called Gödel Number Sequence (GNS) using a new technique called Godelization. Digital watermarking and Steganography techniques are used to address these types of problems like protecting information and concealing secrets. As these techniques suffer from various limitations, we use Godelization technique.

Keywords: *Alphabetic coding, Gödel number, Gödel Number Sequence (GNS).*

1. Introduction

1.1 Security Issues:

- **Confidentiality** is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right
- people can in fact get it Access must be restricted to those authorized to view the data in question.
- **Integrity** involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Integrity of information refers to protecting information from being modified by unauthorized parties.
- **Authentication** is the process of identifying an individual, usually based on username and password. In security systems, authentication is distinct from authorization , which is the process of giving individuals access to system objects based on their identity.

The project entitled **"An innovative loom for secure diffusion of Images"** is a form of transmitting an image in a secure way. The image is taken in to consideration and the intensity values of that image are read. The intensity values are converted to the Gödel number sequence. As the input is large in data, they are compressed using different Data compression algorithms for reducing the data. The compressed data is given to any Symmetric Encryption algorithm and is encrypted using a public key. At the Decoding end, the encrypted data is decrypted using public key and the decrypted data is given as input to the data compression algorithm to get the original data. At the last stage we recover back the original image.

- **Confidentiality** is the property of protecting the content of information from all users other than those intended by the legal owner of the information. The non intended users are generally called unauthorized users.
- **Integrity** is the property of protecting information from alteration by unauthorized users. Availability is the property of protecting information from non authorized temporary or permanent with holding of information.
- **Authentication** means identifying origin of message correctly and it should ensure that identity is not false.

ISSN 2348 – 7968

1.2. Password Authentication:

Password authentication [PA] is one of the simplest and the most convenient authentication mechanisms to deal with secret data over networks. It is more frequently required in areas such as computer networks, wireless networks, remote login systems, operation systems and database management systems. The use of passwords is the primary means of authenticating a user.

1.3. Godelization:

The logician Kurt Gödel developed an encoding scheme to assign numbers to statements and formulas in an axiomatic system which is based on prime factorization method. According to the proposed **Godelization** method, it is a process of converting any positive integer which is greater than 1 into a sequence called Gödel Number Sequence (GNS). For any positive integer n>1, define GNS (n) = $(x^0, x^1 \ldots. x^k)$ where n= $2^0 * 3^1 * 5^3 \ldots p^{x^k}$) is the prime factorization of n. For example GNS(198) = (1,2,0,0,1) because 198 = $2^1 * 3^2 * 5^0 * 7^0 * 11^1$. Although Gödel Numbering has been used for many applications, we use this scheme for encoding of digital images. Every digital image can be viewed as a sequence of intensity values ranging from 0 to 2m - 1 for some positive integer m. Thus if any image is represented by intensity values $(i_1, i_2, \ldots i_n)$ then each of these intensity values can be converted into a Gödel Number Sequence (GNS). Then GNS (i_1) $GNS (i_2) $.....$GNS (i_n) is called the Gödel String of the image.

1.3.1 Encoding the Image into Gödel Number Sequence:

- Gödel numbering is a function that assigns to each symbol or a set of sequence of numbers, a unique natural number called “Gödel number”.
- For a sequence of numbers $a_1, a_2, a_3, \ldots. a_n$; the Gödel number written $(a_1, a_2, a_3, \ldots. a_n)$ is defined as $[a_1, a_2, a_3, \ldots. a_n] = p_1^{a_1} * p_2^{a_2} * p_3^{a_3} \ldots p_n^{a_n}$ where ‘a’ refers to arbitrary numbers and ‘p’ refers to prime numbers.
- Sample: G 4 3 1 Then the Gödel number of it can be written as $2^4 * 3^3 * 5^1 = 16 * 27 * 5 = 2160$.

1.3.2 ASCII BIT ENCODING Algorithm:

This is a process of compressing a given string of numbers. If an image has N intensity values then the Gödel String consists of the digits 0 to [log2N](apart from $ symbol).Normally N will be 255 and hence the Gödel string of any image will have numbers ranging from 0 to 7. If 3 or more characters are encountered in a sequence, then it is represented as KX where k is the number of occurrences of character X. So the string $100000001$0200000001 is encoded as 1$70111$10127011 Here the length is reduced to 16 bytes from 21 bytes.

1.3.3 LEMPEL-ZEV-WELCH (LZW) Algorithm:

Lempel–Ziv–Welch (LZW) is a universal lossless data compression algorithm created by Abraham Lempel Jacob Zev, and Terry Welch. It was published by Welch in 1984 as an improved implementation of the LZ78algorithm published by Lempel and Zev in 1978. The algorithm is simple to implement, and has the potential for very high throughput in hardware implementations. It was the algorithm of the widely used UNIX file compression utility compress and is used in the GIF image format. The scenario described by Welch encodes sequences of 8-bit data as fixed-length 12-bit codes. The codes from 0 to 255 represent 1-character sequences consisting of the corresponding 8-bit character, and the codes 256 through 4095 are created in a dictionary for sequences encountered in the data as it is encoded. At each stage in compression, input bytes are gathered into a sequence until the next character would make a sequence for

ISSN 2348 – 7968

which there is no code yet in the dictionary. The code for the sequence (without that character) is added to the output, and a new code (for the sequence with that character) is added to the dictionary. LZW uses fixed-length code words to represent variable-length strings of symbols/characters that commonly occur together. The LZW encoder and decoder build up the same dictionary dynamically while receiving the data.

TABLE 1.3.3(1) Initial LZW Dictionary

Index	Entry
1	$
2	a
3	b
4	o
5	w

TABLE 1.3.3(2) Constructing the 12th Entry of LZW Dictionary

Index	Entry
1	$
2	a
3	b
4	o
5	w
6	wa
7	ab
8	bb
9	ba
10	a$
11	$w
12	w…

TABLE 1.3.3(3) Final LZW Dictionary for the Given Input

Index	Entry
1	$
2	a
3	b
4	o
5	w
6	wa
7	ab
8	bb
9	ba
10	a$
11	$w
12	wab
13	bba
14	a$w
15	wabb
16	ba$
17	$wa

ISSN 2348 – 7968

18	abb
19	ba$w
20	wo
21	oo
22	o$
23	$wo
24	oo$
25	$woo

Encoder output sequence

5 2 3 3 2 1 6 8 10 12 9 11 7 16 5 4 4 11 21 23 4

1.3.4 DATA ENCRYPTION STANDARD (DES):

The **Data Encryption Standard** (**DES**) is a predominant symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world. It was developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data.

2. Proposed System

The Proposed technique is a secured way of transmitting image which eliminates the drawbacks of the Existing system. The proposed technique involves three stages.

2.1 Proposed Technique:

- The first stage consists of encoding the image into a Gödel String.
- In the second stage the Gödel string is compressed using several Data compression techniques and the compression ratios of each algorithm will be calculated.
- The Compression ratios of each algorithm are compared and the data obtained from the algorithm with better compression ratio is given as input to the next stage.
- In the third stage, the compressed string will be encrypted using a symmetric key cryptosystem or a public key Cryptosystem.
- At the decoding end again there will be three stages to recover back the image which is the reverse process of the above three.

3. SYSTEM IMPLEMENTATION

3.1 Matlab:

MATLAB was developed primarily by Cleve Moler in the 1970's and is derived from FORTRAN subroutines LINPACK and EISPACK, linear and Eigen value systems. It was developed primarily as an interactive system to access LINPACK and EISPACK and gained its popularity through word of mouth, because it was not officially distributed. It was rewritten in C in the 1980's with more functionality, which includes plotting routines. The Math Works Inc. was created (1984) to market and continue development of MATLAB.

The Matlab is implemented in this project by using some functions like; Images are read into the MATLAB environment using function imread. Images are displayed on the

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 11, November 2015.
www.ijiset.com
ISSN 2348 – 7968

MATLAB desktop using functions imshow and imtool. Images are written to the Current Directory using function imwrite and etc.

4. Results

Fig: **- 4.1** Screen Showing the Input Image

Reading the Intensity Values of an Image:

Fig: - 4.2. Screen Showing the Intensity Values of an Image

Encoding the Intensity Values to Godel Number Sequence:

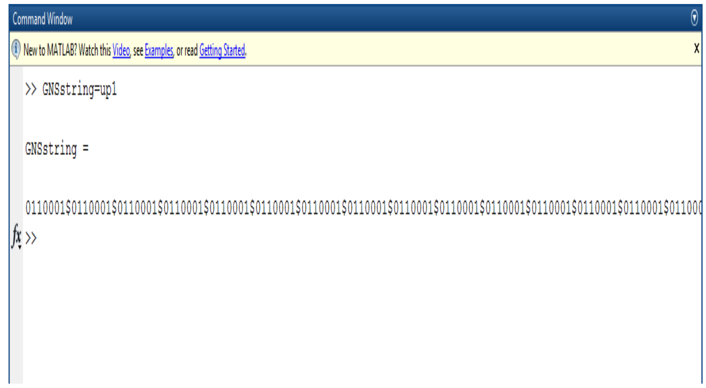

Fig: - 4.3. Screen Showing the Gödel Number Sequence.

Compression using ASCII bit Encoding:

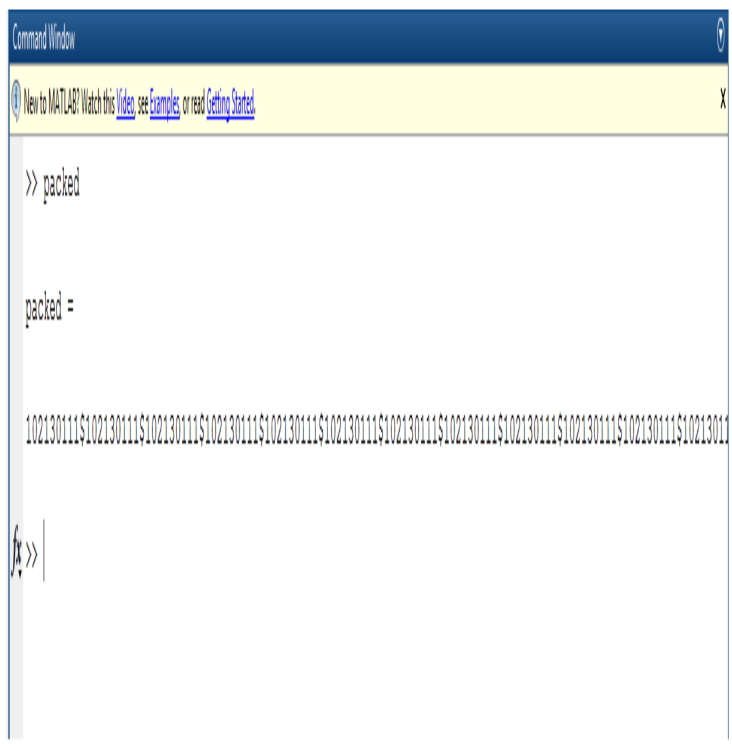

Fig:- 4.4. Screen Showing the Compressed Data Using ASCII bit Encoding

ISSN 2348 – 7968

Comparing the Size of String Before and After Compression by ASCII bit Encoding:

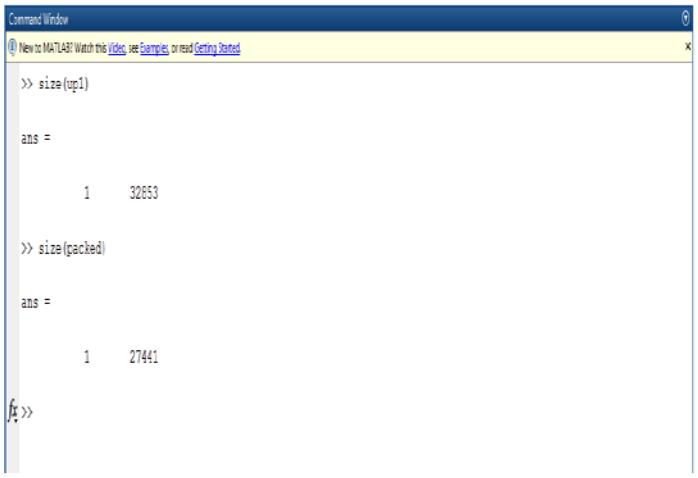

Fig: -4.5. Screen Showing the Size of the String Before and After Compression by ASCII Encoding

Compression ratio by ASCII bit Encoding:

Fig: - 4.6. Screen Showing the Compression ratio Obtained by Using ASCII bit Encoding.

Compression Using LZW Algorithm:

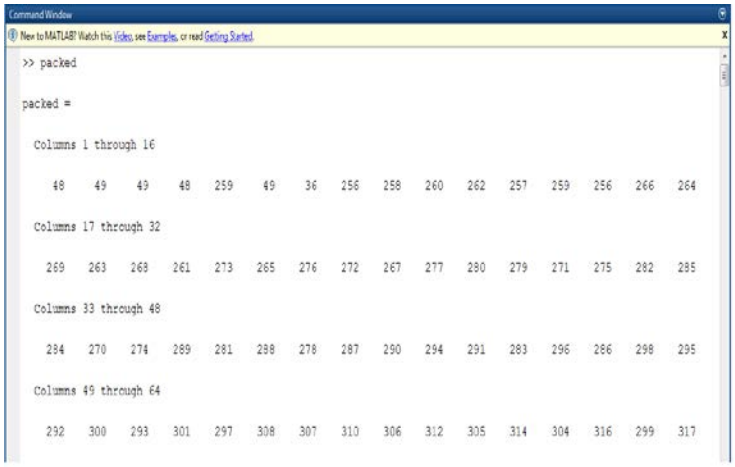

Fig: -4.7. Screen Showing the Compressed String Using LZW Algorithm

Comparing the Size of String Before and After Compression:

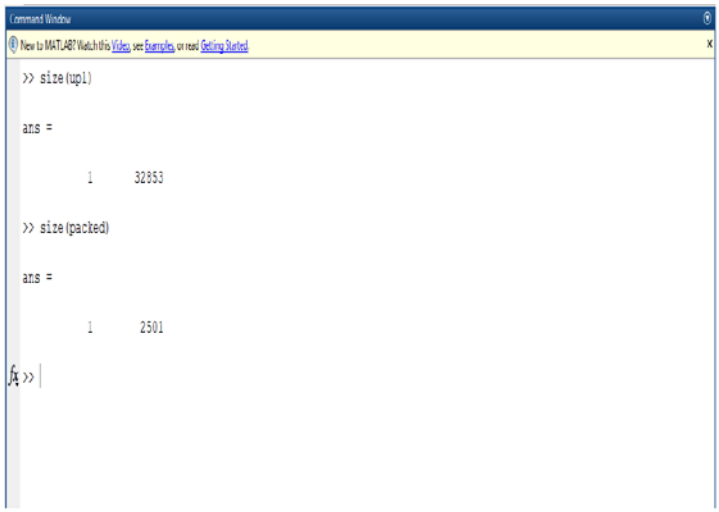

Fig: - 4.8. Screen Showing the Size of the String Before and After Compression

Compression ratio by LZW Algorithm:

ISSN 2348 – 7968

Fig: - 4.9. Screen Showing the Compression ratio Obtained by Using LZW Algorithm

Encrypted String:

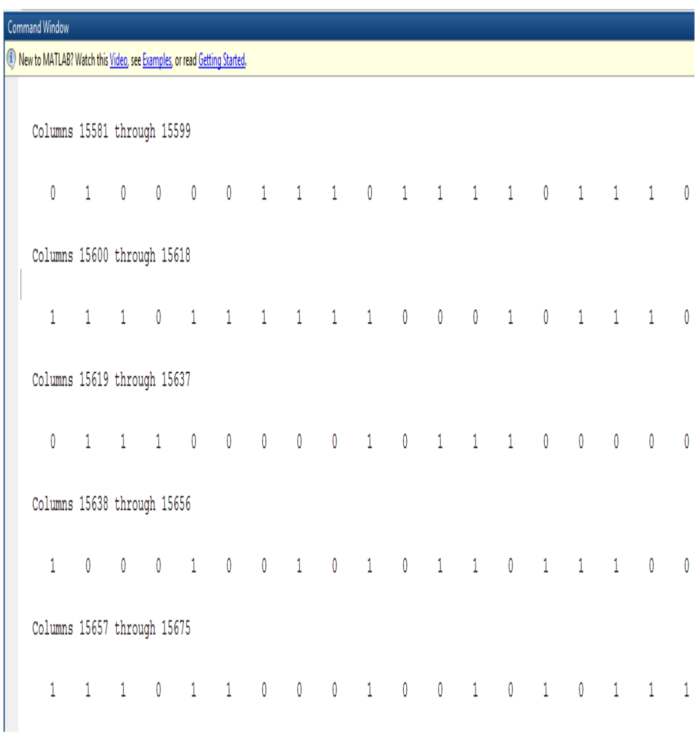

Fig: - 4.10. Screen Showing the Encrypted String.

Decrypted String:

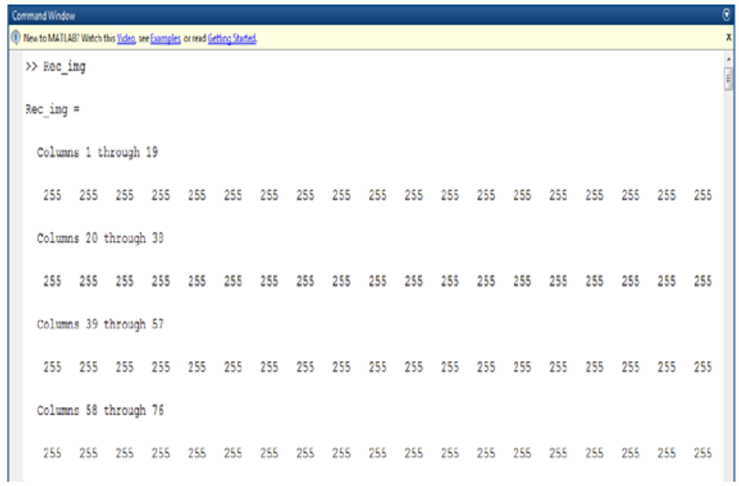

Fig: - 4.11 Screen Showing the Decrypted String

Decompressing the String by LZW Algorithm (LZW Decoding):

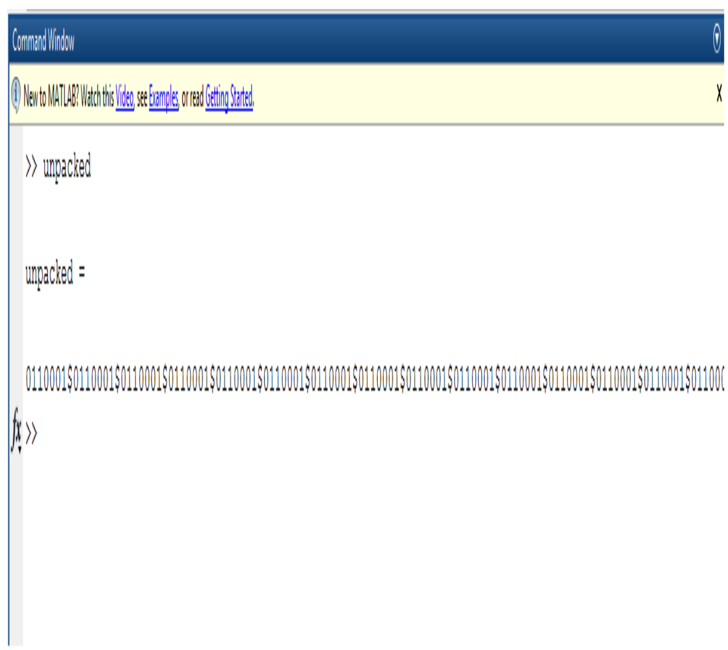

Fig: - 4.12 Screen Showing the Decompressed String

Inverse Godelization:

ISSN 2348 – 7968

Fig: - 4.13 Screen Showing Inverse Godelization.

5. Conclusion:

The Internet has become so user friendly that it has become an excellent distribution system for digital media. There exists several techniques which play a significant role in the field of security but they suffer from few limitations. In this project, a new model for transmitting an image securely using a technique called Godelization is proposed. This method is implemented using Encoding and Decoding methods. Experimental results show that the proposed method works efficiently for images and as well as for text, while for large images Godelization requires some processing time which is not a big concern with the available hardware support today. This method proves to be secure and efficient as two layers of encoding will be provided.

REFERENCES

[1] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., "Information hiding
– A survey", Proc. of IEEE, Vol.87, No.7, 1999, pp.1062-1078.

[2] D.LalithaBhaskari, P.S.Avadhani, A.Damodaram, "A Combinatorial
Approach for Information Hiding Using Steganography And Godelization Techniques", IJSCI (International Journal of Systemics,
Cybernetics and Informatics), ISSN 0973-4864, 2007, pgs 21-24.

[3] John Martin, "Introduction to Languages and the theory of
Computation", 3rd edition, TMH, pp no.462.

[4] W. Diffie & M. Hellman, "New directions in cryptography", IEEE
Trans. Information Theory, Vol.22, 1976, pp. 644-654.