A New Encryption Method for Secure Transmission of Images

B.V.Rama Devi
Research Scholar, Dept. of CS&SE,
Andhra University, Visakhapatnam

P.Prapoorna Roja
Dept. of I.T., SSN Engineering College
Chennai

D.Lalitha Bhaskari
Dept. of CS&SE,
Andhra University ,Visakhapatnam

P.S.Avadhani
Dept. of CS&SE, Andhra University,
Visakhapatnam

Abstract -In this paper, a novel approach is designed for transmitting images securely using a technique called Gödelization followed by the public key encryption. The image which is to be transmitted is transformed into a sequence called Gödel Number Sequence (GNS) using a new technique called Gödelization. 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.

Key Words: Alphabetic coding,Gödel Number Sequence(GNS), Public key Encryption

1. INTRODUCTION

With the rapid expansion of the Internet and overall development of digital technologies there is a dire necessity for robust methods which provide greater security in handling digital content especially images. Digital watermarking and Steganography techniques are used to address these types of problems like protecting information and concealing secrets. However these techniques suffer from various limitations[1]. This paper proposes a novel methodology to overcome a few limitations by converting the image into a

Gödel Number Sequence and transmitted securely using encryption methods.

2. BASIC CONCEPTS

There are basically three modules in the proposed method, namely the conversion of the image into a string of Gödel Number Sequence(also called the Gödelization),the alphabetic coding and the encryption proceeds. In this section a brief description of the definitions and the concepts of these three modules which are being used in the later part of the paper are presented.

2.1 Gödelization: The logician Kurt Gödel [3] 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 *Gödelization* 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) = $(x_{0,}x_{1,......}x_k)$ where n= $2^{x0} * 3^{x1} * 5^{x3} \dots P^{xk}$ 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 2^m - 1 for some positive integer m. Thus if any image is represented by intensity values$(i_{1,}\ i_{2,.......}\ i_n)$, then each of these intensity values can be converted into a Gödel Number Sequence GNS[2]. Then $GNS(i_1)\$GNS(i_2)\$......\$GNS(i_n)$ is called the Gödel String of the image.

2.2 Alphabetic Coding(AC): 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 [$\log_2$N](apart from \$ symbol).Normally N will be 255 and hence the Gödel string of any image will have numbers ranging from 0 to 7. Now 0,1,…,7 are replaced by A,B,….,H. 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 \$B7AB\$AB7AB\$. Here the length is reduced to 12 bytes from 21 bytes. With AC technique the length is reduced as well as second level of security is also provided.

2.3 Encryption: This is a process of encoding a given text or a string into an unintelligible format. There are two types of encryption methods being used in literature, namely Symmetric Encryption and the Public Key Encryption[4]. In symmetric key encryption the sender uses a key (a secret string) to encrypt the message which upon receiving at the other end will be decrypted using the same secret key. That is, the secret key is known only to the sender and the receiver. However, in public key cryptography, both sender and the receiver will have two keys namely the public key and the private key. The sender encrypts the message using the receiver's public key and the receiver will decrypt it using his private key. Although any of the two methods may be used, in the proposed work symmetric key cryptography is adopted.

3 .PROPOSED METHOD

The proposed technique involves three stages. The first stage consists of encoding the image into a Gödel String. In the second stage the Gödel string is compressed using Alphabetic coding which in the third stage 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 are the reverse process of the above three. The encoding, decoding algorithms and the schemes are given in the following sections.

3.1 Algorithm for Gödelization

The given image is converted to a Gödel string using the following algorithm.

Step 1: Read the intensity values of the
input image.

Step 2: Generate the Gödel String of the
image.

Step 3: Compress the Gödel String using
Alphabetic coding technique.

Step4: Encrypt the string obtained in
step 3 using an symmetric key crypto
system[4] with key K.

This encrypted string is transmitted to the other end. The scheme of the proposed encoding methodology is shown in Fig 1.

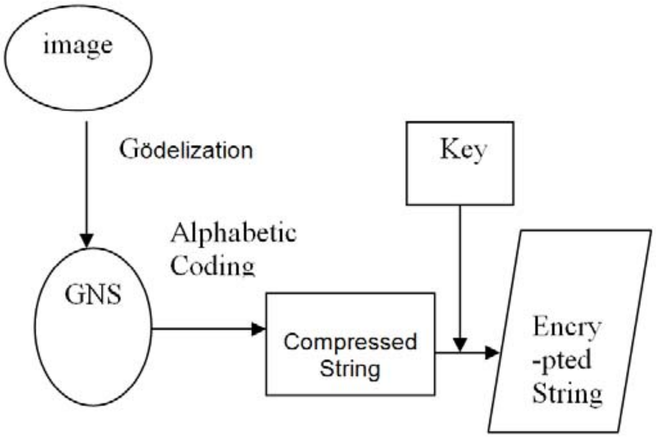


Fig1. Scheme for Gödelization Process

3.2 Inverse Gödelization & Inverse Alphabetic Codingtechniques

At the decoding end, there is a need to perform the inverse operations of Alphabetic coding and Gödelization techniques to obtain the original data. Inverse Alphabetic coding is the process of decompressing the string by replacing alphabets(A,B,…H) with digits(0,1,…7) and any substring KX is decompressed with K occurrences of X. The string obtained is in the form of $GNS(i_1)\$GNS(i_2)\$......\$GNS(i_n)$ which is the Gödel String of the image and inverse Gödelization is applied to the string to obtain the intensity values of the image which are calculated as $GNS(i) = (x_{0,}x_{1,......}x_k)$ where $i= 2^{x0} * 3^{x1} * 5^{x3}…. P^{xk}$.

3.3 Algorithm for Decryption

Once the encrypted form of the image is received, the image can be reconstructed using the following algorithm:

Step 1: Decrypt the received string using the same symmetric key crypto system with the key K.

Step 2: Decompress the string using inverse Alphabetic Coding.

Step 3: Use inverse Gödelization for the string obtained in step 2 to get the intensity values of the image.

Step 4: Construct the image with the values obtained in step 3.

The scheme of the proposed decryption methodology is shown in Fig 2.

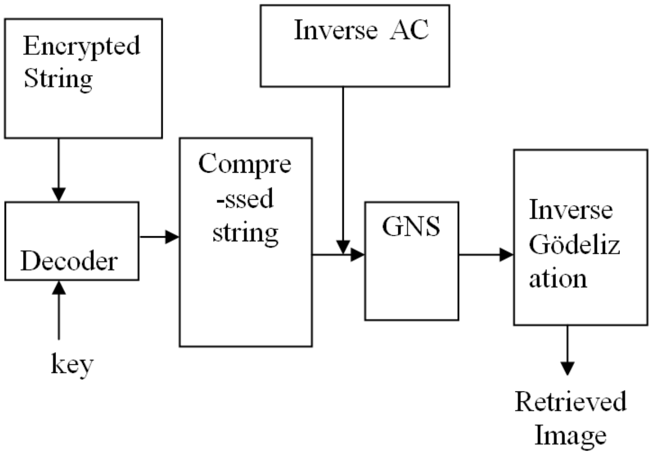
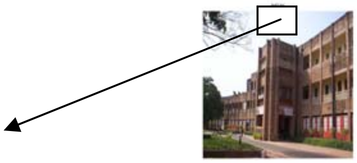


Fig 2. Scheme for decoding

4. Results

Test cases are generated for images with intensity values ranging from 0-255 and for generating symmetric key DES is used.



178 171 155 110 43 30

186 178 165 128 66 172

194 182 171 147 94 32 01

198 183 171 158 114 42 10

204 190 175 165 130 55 1

210 202 184 173 146 72 12

207 208 190 176 154 83 19

Each intensity value of the image is taken and Gödel Number sequences are generated and each sequence is delimited by $ to get Gödel Number String of the image as given below.

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 $ 0
2 0 0 0 0 0 1 $ 0 0 1 0 0 0 0 0 0 0 1 $ 1 0 1 0 1
$ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 $ 0 1 $ 10 $ 1 1 0
0 0 0 0 0 0 0 1 $ 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 1 $ 0 1 1 0 1 $ 7 $ 1 1 0 0 1 $ 0 0
0 0 0 0 1 $ 1 $ 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 1 $ 1 0 0 1 0 1 $ 0 2 0 0 0 0 0 1 $
0 1 0 2 $ 1 0 0 0 0 0 0 0 0 0 0 0 0 0 1 $ 5 $ 11
$ 1 2 0 0 1 $ 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
$ 0 2 0 0 0 0 0 1 $ 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 1 $ 1 1 0 0 0 0 0 1 $ 1 1 0 1 $ 10 $
2 1 0 0 0 0 1 $ 1 0 1 0 0 0 0 1 $ 0 0 2 1 $ 0 1 1
0 1 $ 1 0 1 0 0 1 $ 0 0 1 0 1 $ 11 $ 1 1 1 1 $ 1
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
$ 3 0 0 0 0 0 0 0 1 $ 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 $ 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 $ 3
2 $ 2 1 $ 0 2 0 0 0 0 0 0 1 $ 4 0 0 0 0 1 $ 1 0 1
0 0 0 0 1 $ 4 0 0 0 1 $ 1 0 0 1 1 $ 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 $ 0 0 0 0 0 0 0 1
$

As it is observed that there are repetitions of digits, Alphabetic coding is applied to the above string to obtain the compressed form which is as shown below.

B 22 A B $ A C 5 A B $ 2 A B 7 A B $ B A B A B $ 13 A B
$ A B $ X $ 2 B 8 A B $ B 22 A B $ A 2 B A B $ H $ 2 B 2
A B $ 6 A B $ B $ B 23 A B $ B 2 A B A B $ A C 5 A B $
A B A C $ B 13 A B $ F $ Y $ B C 2 A B $ A B 15 A B $ A
C 5 A B $ B 20 A B $ 2 B 5 A B $ 2 B A B $ X $ C B 4 A B
$ B A B 4 A B $ 2 A C B $ A 2 B A B $ B A B 2 A B $ 2 A
B A B $ Y $ 4 B $ B 24 A B $ D 7 A B $ 39 A B $ B 19 A B
$ D C $ C B $ A C 6 A B $ E 4 A B $ B A B 4 A B $ E 3 A
B $ B 2 A 2 B $ 22 A B $ 7 A B $.

The length of the GNS sequence is 498 and the length of the compressed string is 236 where we have achieved nearly 50% compression. There is a considerable amount of compression when compared. Now the above data (encoded and compressed string) is encrtpted using any public key encryption techniques and a key will be generated. This key will used at the decoding end to retrieve the encrypted data first, then inverse process of Alphabetic coding will be applied and then inverse Gödelization will be applied
to retrieve the data, from which the image will be reconstructed. After decoding the
retrieved image is as shown and we can observe that there is no distortion in the retrieved image.

Original Image

Retrieved Image

5. Conclusions & Future Work

A new model for transmitting an image securely using a technique called Gödelization is proposed. Experimental results show that the proposed method works efficiently for images and as well as for text, while for large images

Gödelization 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.

6.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 GÖdelization Techniques”, IJSCI (International Journal of Systemics, Cybernatics 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.

About Authors:

B.V. Rama Devi comleted her Masters Degree in Computer Science and Technology in 1998 from Andhra University, Visakhpatnam. She has been in software industry since 1998. She worked as a software Developer from 1998 till 2004 in Computer Science Unit, IIT Delhi, New Delhi and has extensive knowledge in INGRES RDBMS, INGRES DBA, UNIX, Shell Scripting and C. She has worked in large teams and presently handling the responsibility of Project Leader in Ms Steria. Has been awarded “PAT ON THE BACK” by Ms Steria several times. Has completed ITIL Foundation Certification.

P.Prapoorna roja is working as a professor in Dept. of IT ,S.S.N.College of engineering , chennai. She has a total of 15 years of teaching experience and has a number of paper publications in both national/international journals and conferences. Her areas of interest include networks, cryptography, database security.

Dr.D. Lalitha Bhaskari is currently working as Associate Professor in the department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam. Her areas of interest include Digital Watermarking, Data Security, Image Processing, Data communications, Pattern Recognition. Apart from her regular academic activities she holds responsibilities like Associate Member in the Institute of Engineers, Member-CSI, Associate Member in the Pentagram Research Foundation, Hyderabad, India. She is also the recipient of “Young Engineers Award” for the year 2008 from the prestigious Institution of Engineers(INDIA). She has 12 years of teaching experience and several publications in various international journals and conferences.

Dr. P. S. Avadhani is a Professor, in the department of Computer Science and Systems Engineering of Andhra University.He is also the Chairman BOS and Placement officer for AUCE(A),Andhra University.He has guided one Ph. D student and right now he is guiding 10 Ph. D Scholars from various institutes. He has guided more than 93 M.Tech. Projects. He received many honors and he has been the member for many expert committees, member of Board of Studies for various universities, Resource person etc for various organizations. He has co-authored 4 books. He is a Life Member in CSI, AMTI, ISIAM, ISTE, YHAI and in the International Society on Education Technology. He is also a Member of IEEE, and a Member in AICTE.