

# A Secured Approach for Watermark Embedding using Key based Gödelization Technique under Spatial and Frequency Domains

P. Raja Mani

Department of Computer Science Engineering,  
GITAM University Visakhapatnam,  
Andhra Pradesh, India

D.Lalitha Bhaskari

Department of Computer Science and Systems  
Engineering, AUCE(A), Andhra University  
Visakhapatnam, Andhra Pradesh, India

## ABSTRACT

The huge availability of multimedia data on the internet makes the creation, modification and distribution of the multimedia content easy and affordable. This improvement in the digital techniques has led a path to unauthorized access, copying and distribution of multimedia data, which throws a serious challenge in the field of copyright protection. This paper focuses on providing security and authentication through a method termed Gödelization for the purpose of encryption and Location Decision Embedding Technique(LDET) for multimedia data embedding.

## General Terms

Data Hiding

## Keywords

Gödelization, Spatial Domain, Frequency domain, Haar Wavelet Transform.

## 1. INTRODUCTION

Security of data over Internet is a great challenge. To accomplish Data Security and build such systems, several Data hiding techniques exist. Data hiding is a technique of embedding a sequence of bits on a cover image with small visual deterioration and the means to extract it afterwards. This is a technique to insert particular data into an image, in order to detect later any accidental or malicious alterations in the image, as well as to certify that the image came from the right source. There are many embedding techniques which can be classified based on the domain as spatial domain[1] and frequency domain[2]. The techniques in both of these domains have their own advantages and disadvantages. Spatial Domain techniques embed data into the pixels of the Cover Image directly which has very low computational complexity. So the proposed approach embeds the watermark image in Spatial Domain. Frequency domain schemes are more robust to tampering and attacks than those in Spatial Domain. But a less amount of data can be embedded in Frequency Domain when compared to Spatial Domain. So Frequency Domain is chosen to embed the Key, as the Key has to be transmitted more securely without which data cannot be extracted. This also acts as a second level of Authentication. In addition the Frequency Domain, discrete wavelet transform(DWT) has good time-frequency features and accurate matching of the human visual system(HVS).

In the next section Spatial and Frequency Domain techniques are explained clearly. Section III focuses on the details of the embedding and extracting algorithms. Sections IV and V

show experimental results and observations. Section VI deals with the conclusion and future work followed by references.

## 2. TYPES OF WATERMARKING

### 2.1 Spatial Domain Watermarking

In the spatial domain watermarking, the pixels comprising of image details are considered and the various procedures are directly applied on these pixels. The image processing functions in the spatial domain may be expressed as

$$g(x, y) = T[f(x, y)] \quad (1)$$

where  $f(x, y)$  is the input image,  $g(x, y)$  is the processed output image and  $T$  represents an operation on ' $f$ ' defined over some neighborhood of  $(x, y)$ . Sometimes  $T$  can also be used to operate on a set of input images. In Spatial domain, different methods are used for watermarking. Some of the methods are as follows:

#### 2.1.1 Correlation based Technique

In this technique a pseudo random noise pattern is applied to the image and the correlation between the noise pattern and the watermarked image is exploited [12].

#### 2.1.2 LSB Embedding

This technique has the advantage of simple implementation. It also allows for a relatively high payload, carrying one bit of the secret message per byte of pixel data. In addition, it is also seemingly undetectable by the average human if done right. In addition to being vulnerable to detection techniques, LSB is extremely vulnerable to corruption. That is, the integrity of the hidden message can easily be destroyed[11]. Due to these possible attacks, LSB Embedding is relatively insecure, at least in its primitive form.

In order to protect the integrity of the watermark image a new watermark embedding technique called **Location Decision Embedding Technique (LDET)** is introduced in this approach. This technique is explained in detail in Section III.

### 2.2 Frequency Domain Watermarking

In the frequency domain watermarking, the data is transformed to its frequency representation. In this first the original data is transformed and then modifications are applied to transformed coefficients and inverse transform is applied to recover the data. These techniques distribute the data irregularly over the image pixels after the inverse transform thus making the detection and manipulation of the

data difficult. There are many techniques proposed based on transformation domain. Some of the methods are as follows:

**2.2.1 Discrete Fourier Transform:** These techniques are robust against various attacks, but it is a complex transform.

**2.2.2 Discrete Cosine Transform:** These techniques are weak against rotation, scaling, cropping etc.

**2.2.3 Discrete Wavelet Transform:** This technique decomposes an image into sub images or sub bands, three details and one approximation. The bands are LL, LH, HL and HH. The robustness of the data is increased by embedding into these bands without having additional impact on the quality of the image. The advantage of this technique is that it has multi resolution characteristics. The human eyes are not sensitive to the small changes in edges and textures of an image but are very sensitive to the small changes in the smooth parts of an image. With the DWT, the edges and textures are usually to the high frequency sub bands, such as HH, LH, and HL etc. The major drawback of this method is that the computational requirement is very high as compared to other methods. So Key is embedded in this transform as its size is less and requires less computation. As cited in [9] among the available many watermarking methods in wavelet domain, Haar wavelet is efficient and so it has been used for embedding the key. Figure 1 shows a 2 D digital image "baby" decomposed for Second Level along with the frequency bands

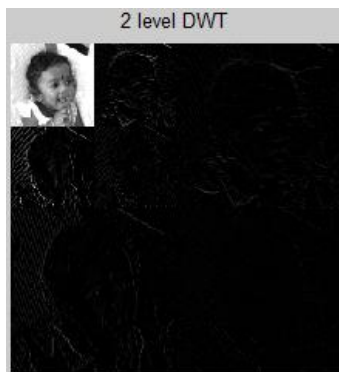


Fig 1 Second Level Wavelet Decomposition

### 3. PROPOSED METHODOLOGY

This section deals with embedding and extracting a watermark image (WM) based on Gödelization[6] earlier proposed by D.Lalitha Bhaskari, P.S.Avadhani, A.Damodaram. In this paper, a methodology is proposed to enhance the security of Gödelization technique by introducing a key and adopting a hybrid approach termed LDET to embed the watermark in the spatial domain and the key into the frequency domain of the cover image.

The secret message or the watermark image(WM) is encrypted using Gödelization technique[6]. As explained by the authors it is a process of converting any positive integer greater than 1 into a sequence called Gödel Number Sequence(GNS). According to it, GNS of 198 is calculated as GNS(1,2,0,0,1). which can be encoded as  $2^1 \times 3^2 \times 5^0 \times 7^0 \times 11^1$ . So now 198 is encoded as 12001. This process is applied for every pixel in the image which is to be hidden. Every pixel is converted into a Gödel Number Sequence as explained above and each of this GNS is added with a private key(K) to

achieve a second level of authentication. Thus the obtained GNS are concatenated to form a Gödel String(GS), where  $GS = GNS(i_1) \$ GNS(i_2) \$ \dots \$ GNS(i_n)$ , n is the number of pixels in the image and \$ is a delimiter. Based on the above procedure, the watermark image obtained after encoding using Gödelization technique is embedded into Cover Image (CI) using Location Decision Technique under Spatial Domain to obtain a Watermarked image(CI'). To enhance the security, the key is embedded in the frequency domain of CI' using Haar decomposition to obtain a Stego image CI''. The results showed that there is no perceptual distortion for CI and CI''.

$$CI'' = CI' + K \quad (2)$$

$$CI' = GNS(WM) \quad (3)$$

In the extraction process, the Stego Image CI'' is decomposed using Haar wavelet for 2 levels to get approximation coefficients, LL2. Key is extracted from the approximation coefficients. Inverse transformation of the wavelet decomposition (IDWT) for 2 levels is applied to obtain the Watermarked image(CI'). The encrypted watermark image is extracted from the Watermarked image(CI') using Location Decision Technique in Spatial Domain. This encrypted watermark image is decrypted using the extracted key and Gödelization technique to retrieve the Watermark Image.

### 3.1 Location Decision Embedding Technique

The Secret data i.e. the watermark is encrypted using Gödelization technique, to which a key is added. A Cover Image (CI) is taken. The encrypted watermark (GS) embedding starts from the seed pixel of CI. The first bit of GS is embedded in the seed pixel at a position indicated by the MSB bit of the seed pixel. A flag is taken and is made 1 to indicate the pixel is visited. The location of the next pixel to be embedded is chosen based on the parity of the embedded pixel. If the parity is even the pixel towards its right in the next row is chosen, else the pixel towards its left in the next row is chosen. Flag of the chosen pixel is checked before embedding. If the flag is 1 it indicates the pixel is already embedded. Then the flag of the pixel in the next column of the same row is verified for embedding. In this way the encrypted watermark is embedded in the Spatial Domain of the Cover Image. This technique protects the integrity of the watermark image with a relatively high payload, carrying one bit of the encrypted watermark per byte of pixel data. In addition, it is perceptually invisible to the human eye.

### 3.2 Embedding Procedure

#### Embedding in Spatial Domain

**Input:** Watermark image(WM) , Cover Image(CI)

**Output :** Watermarked Image(CI') in Spatial domain

- Step 1 :** Calculate Gödel Number Sequence(GNS) of WM image.
- Step 2:** Concatenate these sequences delimited by \$ to form a Gödel String.
- Step 4 :** Key(K) is generated and added to each of the GNS calculated in step 2.
- Step 5 :** The GS is obtained by concatenating all GNS and is embedded using LDET.

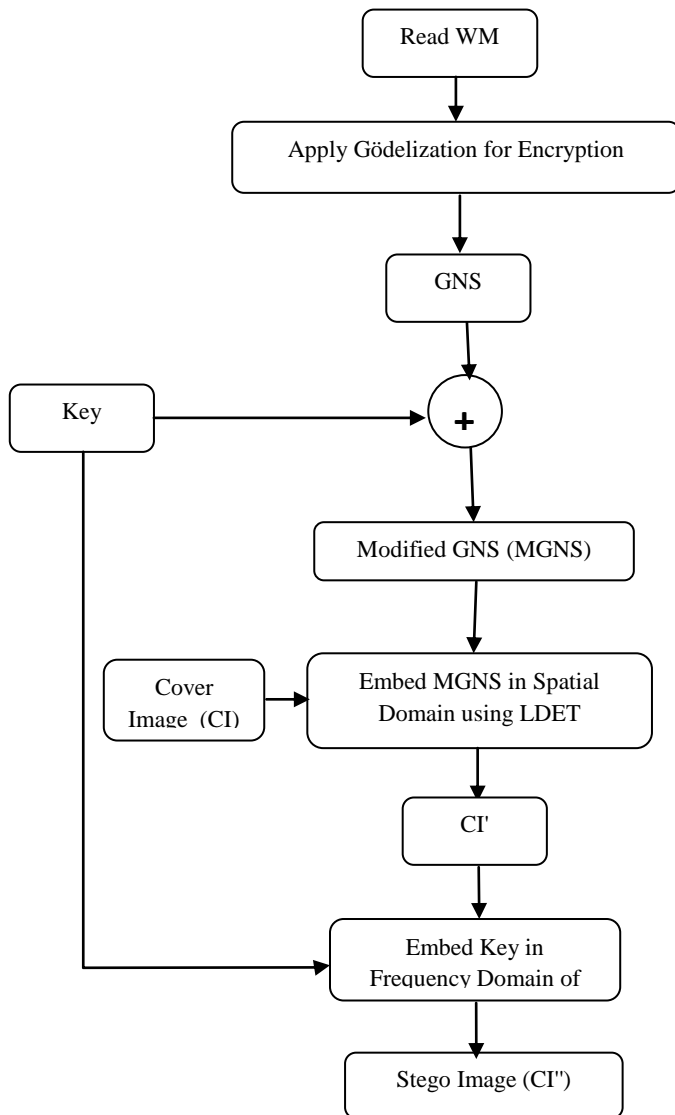


Fig 2. Watermark Embedding

**Step 6 : Location Decision Embedding Technique**

- 6.1: Cover Image CI of size(M,N) is considered.
- 6.2: A seed pixel of CI which is kept secret, is taken as the starting location for embedding the first bit of the GS.
- 6.3: The first bit of GS is embedded in the seed pixel at a position indicated by the MSB bit of the seed pixel.
- 6.4 If the MSB == 1 then the bit is embedded in the LSB+1 position else the bit is embedded in LSB position.
- 6.5: A flag is made 1 to indicate the pixel is visited.
- 6.6: The location of the next pixel in which the next bit is to be embedded is chosen based on the parity of the already embedded pixel. If the parity is even

the pixel towards its right in the next row is chosen, else the pixel towards its left in the next row is chosen.

6.7: Visited flag bit of the chosen pixel is checked before embedding. If the flag is 1 it indicates the pixel is already embedded. Then the flag of the pixel in the next column of the same row is verified for embedding.

Repeat from step 6.4 until all the bits are embedded

**Embedding in Frequency Domain**

**Input :** Watermarked Image(CI') obtained from step 6

**Output:** CI''(where CI'' = CI' + Key ) in frequency domain

- Step 7 : Now the Watermarked image(CI') is decomposed using Haar wavelet for 2 levels to get approximation coefficients, LL2.
- Step 8: The key is embedded in the approximation coefficients.
- Step9: The inverse transformation of the wavelet decomposition(IDWT) for 2 levels is applied to obtain the Stego Image.

Now the Stego-image contains watermark embedded in Spatial Domain and key embedded in its Frequency Domain. Figure 2 shows the Block Diagram of the Embedding Procedure.

**3.3 Extraction Procedure**

- Step 1: Stego-image is decomposed using 'Haar' wavelet up to 2 levels to get approximation coefficients, LL2.
- Step 2: The key is extracted from approximation coefficients, LL2.
- Step3: Inverse transformation of the wavelet decomposition(IDWT) for 2 levels is applied to get the watermarked image.
- Step 4: Based on the seed pixel the first bit is extracted.
- Step 5: The next bit is extracted from the pixel at a position indicated by the MSB bit of the pixel.
- Step 6: The flag bit is made 1 to indicate the pixel is visited.
- Step 7: The next pixel to be extracted is chosen based on the parity of the extracted pixel. If the parity is even the pixel towards its right in the next row is chosen, else the pixel towards its left in the next row is chosen.
- Step 8 : Visited flag bit of the chosen pixel is checked before extracting. If the flag bit is 1 it indicates the pixel is already extracted , go to step 5 else go to

- step 3
- Step 9 : After extracting the binary string decode it to get the numeric sequence string.
- Step 10 : Deduct the key from each of the Gödel numeric sequence to get the Gödel String.
- Step 11: The Gödel String is decoded to retrieve the Watermark.

Figure 3 shows the Block Diagram of the Extraction Procedure.

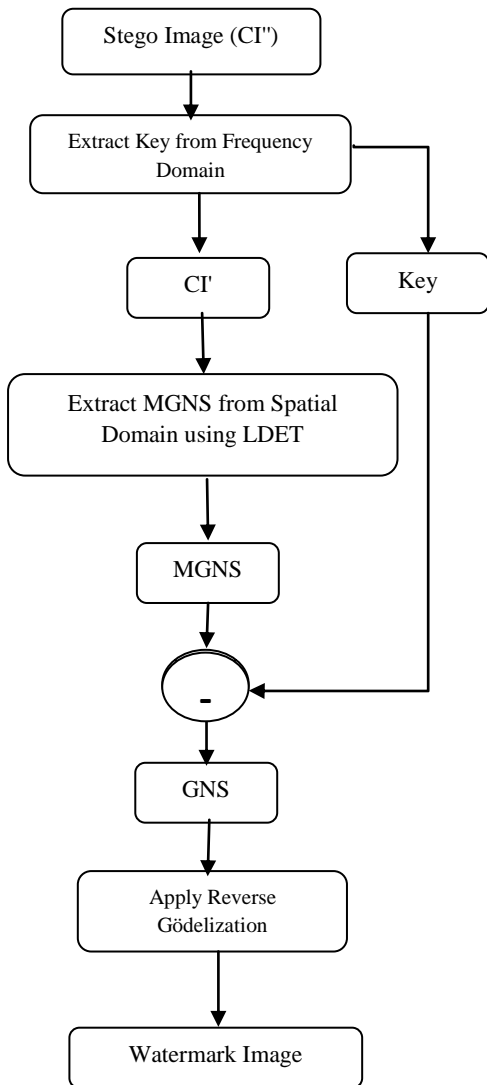


Fig 3. Watermark Extraction

#### 4. EXPERIMENTAL RESULTS

The performance of the proposed approach is evaluated by implementing the proposed approach on 10 standard grey scale images of size 512x512. Figure 4 shows a test image "Butter" and a watermark image "water". Figure 5 shows Cover image, watermarked image along with Stego image. Figure 6 shows Extracted Watermark. The results show the PSNR, MSE for input images i.e "Butter" , "Barbara", "Flight" in Table 1.

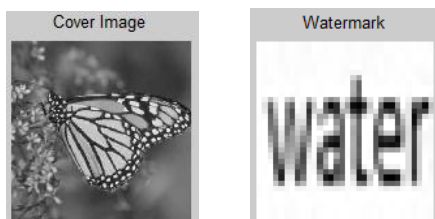


Fig 4. Original Cover Image - Butter and Watermark Image - water

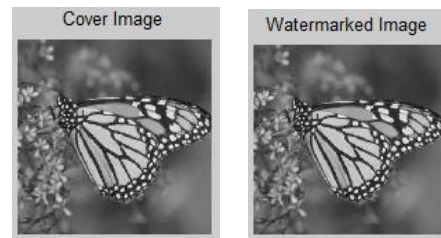


Fig 5. Cover image, watermarked image

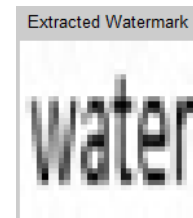










Fig 6. Extracted Watermark

#### 5. OBSERVATIONS

Embedding the Watermark in Spatial Domain involves a very low computational complexity with a high visual quality of the images. Table 1 shows the PSNR of the best test case "butter" with 51.7082. The PSNR of most of the test cases is greater than 50. Nevertheless, the proposed approach is efficient at embedding secret watermark image with a low distortion, while the payload capacity is high. A second level security is achieved by embedding the key in Frequency Domain without any distortions in the image. From the results obtained it is observed that the proposed technique LDET is very efficient in embedding an encrypted watermark.

Table 1 Experimental Results for Standard Images

Cover Image	Watermark Image	PSNR	MSE
 Butter		51.7082	0.4388
 Barbara		50.0292	0.6459
 Flight		48.4906	0.9205
 Baby		51.2368	0.4891

## 6. CONCLUSION AND FUTURE WORK

A hybrid secure data embedding technique is proposed based on Gödelization. The watermark which is encoded using Gödelization is embedded using LDET technique in Spatial Domain where the payload capacity is high. The key is embedded in Frequency domain as it is more robust to tampering and attacks than those in Spatial Domain. The proposed methodology has taken the advantages of both spatial and frequency domains by embedding the watermark in the spatial domain thus increasing the payload capacity. To enhance the security, the key is embedded in the frequency domain to achieve robustness. Even though the attacker could get the key, unless and until the seed pixel is known it is computationally difficult to retrieve the watermark. Thus the proposed hybrid approach of encoding the watermark using Gödelization method and embedding it using LDET technique in spatial domain and embedding the key in frequency domain proves to be efficient.

## 7. REFERENCES

- [1] Schyndel, R.G.V., Tirkel, A.Z., Osborne, C.F., : A Digital Watermark. In: International Conference on Image Processing, vol.2, pp. 86--90. IEEE, Austin, TX, USA (1994)
- [2] Li Li, He-Huan Xu, Chin-Chen Chang, Ying-Ying Ma : A novel image watermarking in redistributed invariant wavelet domain. In : The Journal of Systems and Software 84, pp. 923--929 (2011)
- [3] D. R. Huang, J. F. Liu, and J. W. Huang : A DWT-based Image Watermarking Algorithm. In: Proc of IEEE, ICME, Tokyo, Japan, vol. I, pp. 429--432. (2001)
- [4] Chang-Tsun Li : Multimedia Forensics and Security
- [5] John Martin : Introduction to Languages and the theory of Computation. 3rd edition, TMH, Publications, pp. 462.
- [6] D.Lalitha Bhaskari, P.S.Avadhani, A.Damodaram : A Combinatorial Approach For Information Hiding Using Steganography And Gödelization Techniques. In : International Journal of Systemics, Cybernetics and Informatics (ISSN 0973-4864) pp. 21--24. (2007)
- [7] P. Raja Mani, D.Lalitha Bhaskari : Gödelization and SVD based Image Watermarking under Wavelet Domain In : Proceedings of the International Conference on Frontiers of Intelligence Computing : Theory and Applications pp. 675-681(2012)
- [8] Xiaonian Tang , Quan Wen and Guijun Nian : An Improved Robust Watermarking Technique in Wavelet Domain. In: Second International Conference on Multimedia and Information Technology, pp. 270--273.(2010)
- [9] Liu, J.F., Huang, D.R., Hu, J.Q., : The orthogonal wavelet bases for digital watermarking. In: Journal of Electronics and Information Technology 25(4), pp. 453--459. (2003)
- [10] S. Annadurai; R. Shanmugalakshmi, "Fundamentals of Digital Image Processing"
- [11] Leo Lee, "LSB Steganography Information Within Information Computer Science 265, Section 2 Professor Stamp, April 5, 2004
- [12] C S Rawat, Sneha M Shivamkuty, "A Novel Digital Image Watermarking Using Hybrid Technique " , VESIT , International Technological Conference-2014 (I-TechCON), Jan. 03 – 04, 2014, pp. 181-186