Review on Binary Image Steganography and Watermarking

Mrs. Gyankamal J. Chhajed
VPCOE, Baramati,
Maharashtra, India,
gjchhajed@gmail.com

Ms. Krupali V. Deshmukh
VPCOE, Baramati
Maharashtra , India
krupsdeshmukh@gmail.com

Ms. Trupti S. Kulkarni
VPCOE, Baramati,
Maharashtra , India
truptikvpcoe@gmail.com

***Abstract*-In this paper we have reviewed and analyzed different watermarking and steganography techniques. This is based on image processing in spatial and transform domain. We have reviewed different techniques like data hiding by employing pairs of contour edge patterns, edge pixels, visual distortion tables, visual quality preserving rules, substitution, fixed partitioning of images, run lengths in spatial and using Discrete Cosine Transform, Discrete Wavelet Transform in transform domain. We have also represented analysis of these techniques in the form of table considering different factors of watermarking and steganography like visual quality, embedding capacity, security, robustness and computational complexity. It is concluded that spatial domain techniques are best with some factors like visual quality, while transform domain are best for some factors like robustness against attacks or other image processing operations and security. The data hiding capacity and computational complexity are common factors for both the domains.**

***Keywords*- Watermarking, Steganography, data hiding, data extraction, Information Security, Binary Images, Image Processing.**

I. INTRODUCTION

Today, digital media is getting widely used. It can be digital image, digital audio or digital video. There are a variety of digital media applications like ownership identification, copy control, annotation and authentication.

The digital binary images are widely used in the applications including legal documents, digital books, maps, and architectural and electronic drawings and in business applications. Handwritten signatures captured by electronic signing pads are digitally stored and used as records for credit card payment by many department stores and for parcel delivery by major courier services such as the United Parcel Service (UPS). Word processing software like Microsoft Word allows a user to store his/her signature in a binary image file for inclusion at specified locations of an electronic document. The documents signed in such a way can be sent directly to a fax machine or be distributed across a network. The unauthorized use of a signature, such as copying it onto an unauthorized payment, is becoming a serious concern. In addition, a variety of important documents, such as social security records, insurance information, and financial documents, have also been digitized and stored. Because of the ease to copy and edit digital images, annotation and authentication of binary images as well as detection of tampering are very important. For images in which the pixels take value from only a few possibilities, hiding data without causing visible artifacts becomes more difficult. In particular, flipping white or black pixels that are not on the boundary is likely to introduce visible artifacts in binary images. As these digital media are getting widely used, their security related issues are becoming of primary concern. Hence many digital watermarking techniques have been proposed and very few data hiding techniques are available for binary images.

Watermarking in binary image basically needs identification of locations in image where watermark can be secretly embedded. Hence image processing is a main concern for the same. In images data (watermark) hiding can be done in two domains i.e. spatial domain and transform domain.

The issues of concern related to binary image watermarking are as follows:

1) High embedding capacity
2) Secure watermarking
3) Better visual quality
4) Lower computational complexity
5) Robustness against image processing.

II. IMAGE PROCESSING DOMAINS

A. Spatial domain

In spatial domain, the watermark is embedded by directly altering the pixel values of the original image. One of the simple examples of the spatial domain technique is data hiding using LSB. Most data-hiding techniques for binary images are based on spatial domains, for example, choosing data-hiding locations by employing pairs of contour edge patterns, edge pixels, visual distortion tables and defining visual quality-preserving rules. Recent developments in binary document image watermarking and data hiding techniques includes following:

1. Text Line, Word or Character Shifting
2. Fixed Partitioning of Images
3. Boundary Modifications
4. Modifications of Character Features
5. Modification of Run-Lengths
6. Modifications of Half-Toning Images

B. Transform domain

In transform domain hiding, data are embedded by modulating coefficients in transform domain such as follows:

1. Discrete Cosine Transformation (DCT)
2. Discrete Wavelet Transformation (DWT)
3. Discrete Fourier Transformation (DFT)
4. Discrete Hadamard Transformation (DHT)

Transformed domain watermarking schemes perform the domain transformation procedure by transformation functions such as listed above. Then, the transformed frequency coefficients are modified to embed watermark bits. Finally, the inverse of the corresponding transformation function is performed. The greater parts of the researches embed the watermark in the frequency domain with the purpose improving the robustness. The numerous researches accessible in the literature utilize DWT for watermarking digital images due to its good computational efficiency. Also DWT provides both spatial and frequency resolution. DFT provides only frequency resolution and its time resolution is zero. Hence it is not that much efficient as DWT.

There are several advantages of transform domain embedding over spatial domain embedding. it has been observed that in order for watermarks to be robust, they must be inserted into the perceptually significant parts of an image. For images these are the lower frequencies which can be marked directly if a transform domain approach is adopted. Thus transform domain techniques are robust against attacks. Transform domain techniques have good computational efficiency.

III. WATERMARKING TECHNIQUES

A. *Spatial domain techniques*

a) Using pairs of contour edge patterns

1) *Q. Mei, E. K. Wong, and N. Memon* [1], proposed a data hiding technique for binary text documents in which data are embedded in the 8-connected boundary of a character. They have identified 100 pairs of five-pixel long boundary patterns for embedding data. One of the patterns in a pair requires addition of a foreground pixel adjacent to the center pixel, whereas the other requires the deletion of the center foreground pixel. The 100 pairs of boundary patterns are stored in a lookup table called the *pattern table*s. The embedding is done as follows:

i) The input image is scanned in a left-to-right, and top-to-bottom manner to extract all connected components, which correspond to characters or other symbols in a text document.

ii) Using the first upper-left foreground pixel encountered in the scanning process as the starting pixel an 8-connected boundary following algorithm is used to obtain the closed outer boundary of a connected component. The outer boundary of a character is then traversed in a clockwise manner and divided into a set of consecutive non-overlapping five-pixel-long segments.

iii) The set of consecutive boundary segments is then matched with patterns in the pattern table. If a boundary segment matches a pattern in the pattern table, it is called a *valid boundary segment* which is used for data embedding.

iv) If the data bit to be embedded is a ‘0’ and the current boundary segment is an Add pattern, the pattern is flipped to become a Delete pattern; otherwise no changes are necessary.

v) Similarly, if the data bit to be embedded is a '1' and the current boundary segment is a Delete pattern, the pattern is flipped to become an Add pattern; otherwise, no changes are necessary.
In the extraction process, the same procedure as used in the embedding process is used to extract five pixel long boundary segments from connected components. Valid boundary segments are, again, identified using a table look up procedure and converted to a binary data bits.

Advantages

This method has a good data hiding capacity. If we include inner boundary, the data hiding capacity can be further increased. Since the method hides data in non-smooth portions of text character boundaries, alterations are hardly noticeable. The duality property of the Add-Delete patterns allows easy extraction of hidden data without complicated enforcing techniques, and without referring to the original document.

Limitations

This technique is not robust to printing and scanning and hence is useful only in steganography and authentication applications.

b) Using edge pixels

1) *Yu-Chee Tseng et al.* [2], proposed a data hiding technique for 2-color images in which quality of the image after hiding is considered. It ensures that, for any bit that is modified in the host image, the bit must be adjacent to another bit that has the same value as the former's new value. Thus, the existence of secret information in the host image is difficult to detect. The embedding process is as follows:
Given an image F it is partitioned into locks of fixed size. Let F_i represents the block in the image, K represents the randomly selected binary matrix and W is a weighted matrix.

If F_i is completely black or blank, simply keep F_i intact (not hidden with data) and skip the following steps. Otherwise, perform the following:

i) Compute

$$SUM\ ((F_i \oplus K) \otimes W)$$

ii) From the matrix $F_i \oplus K$, compute for each w=1…2^{r+1}-1 (where r is the number of bits to be embedded) the following set:

$$S_w^{'} = \{(j,k) \mid [([W]_{j,k} = w) \wedge ([F_i \oplus K]_{j,k} = 0) \wedge ([dist(F)]_{j',k'} \le \sqrt{2})]$$
$$\vee [([W]_{j,k} = 2^{r+1} - w) \wedge ([F_i \oplus K]_{j,k} = 1) \wedge ([dist(F)]_{j',k'} \le \sqrt{2})]\}$$

iii) Define a weight difference

$$d' = (b_1 b_2 ... b_r 0) - SUM((F_i \oplus K) \otimes W) (\mathrm{mod}\ 2^{r+1})$$

iv) If d'=0, there is no need to change F_i .Otherwise randomly select matrix indices from S_w to increase the SUM by w.

Advantages

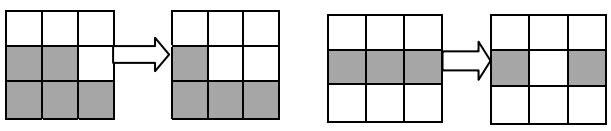
Because of the good quality of the image after hiding data, the existence of secret information in the host image is difficult to detect and hence this scheme is secure.

Limitation

Data hiding space is to sacrificed to achieve good quality of the image after hiding.

c) Using visual distortion table

1) *Wu and Bede Liu* [4], proposed a data hiding technique for binary image authentication in which image is partitioned into blocks and a fixed number of bits are embedded in each block by changing some pixels in that block. Pixels with high flippability scores are used for data hiding. Shuffling is applied to equalize uneven embedding capacity. The embedding is done as follows:
i) Compute Smoothness and Connectivity Measures of 3 × 3 Patterns where the smoothness of the neighborhood around pixel is measured by the total number of transitions along four directions in the 3 × 3 window and the *connectivity* is measured by the number of the black and white clusters.



(a) (b)

Fig1: Example, flipping the center pixel to white in (a) is less noticeable than that in (b).

ii) Flippability scores are determined dynamically by observing the smoothness and connectivity. The pixels with high flippability scores will be used for embedding the data.
iii) To embed a "0" in a block, some pixels are changed so that the total number of black pixels in that block is an even number. Similarly, to embed a "1", the number of black pixels is enforced to an odd number.

Advantages

The hidden data can be extracted without using the original unmarked image. It can also be extracted after high quality printing and scanning with the help of a few registration marks.
This scheme achieves enhanced efficiency by embedding same number of bits in each block.

2) *Gyankamal J. Chhajed et al.* [10] proposed a block based technique for data hiding which uses flappable blocks without enforcing the odd-even features of non-uniform blocks. The length of the data is also preceded to data to be hidden to extract an exact amount of data without need of checking total picture. Authors have identified 17 patterns which can not be used for data hiding as they do not satisfy odd-even feature. Hence this paper proposes the data embedding method without enforcing the odd-even feature in the block. At the time of extraction first the length information is extracted and decoded. Embedding is done as follows:
i) Divide the image in blocks of 3 × 3.
ii) By searching lookup table and finding corresponding node of selected block, the flippability of block is determined for steganography. Blocks with high flippability score used for embedding.
iii) The block is checked for even numbered or odd numbered. If the block is even numbered 1 value is embedded i.e. center pixel should be white after embedding. If center pixel is already white then no change is done.

Advantages

As odd-even feature is not compulsory in this method the number of flippale blocks get increased and hence the capacity.

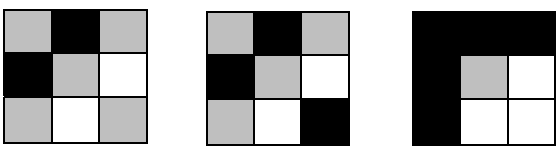
3) *Hae Y. Kim et al*. [5], proposed new cryptography-based secure AWT for binary images that yields good visual quality when applied to binary images including clustered-dot halftones. The embedding process is as follows:
i) Shuffled sequence of given binary image is obtained.
ii)This sequence is divided into two regions. In one region second layer DS is to be stored, while from second region DS is to be computed.
iii) The original non-shuffled image is divided into sub-images.
Each sub-image is pseudo randomly divided into three regions. iv) One region belongs to the first region determined in step 2. In second region first layer MAC is to be stored while from the third region MAC is to be computed.
v) For each shuffled sub-image fingerprint is computed and embedded in it. Also for the whole image fingerprint is computed and embedded in one region.

Advantages

If an image is found to be fraudulent, the owner of the secret-key can spatially locate the alterations to help discovering the intentions of the hacker. Visual quality is excellent.

d) Using visual quality preserving rules

1) *Huijuan Yang et al.* [6], proposed a pattern based data hiding technique for binary image authentication. In this, "connectivity-preserving" criterion is used to assess the "flippability" of a pixel. The criterion is defined based on the observation that if flipping a pixel does not destroy the connectivity among pixels, the visual quality is ensured. In this paper, capacities of different ways to partition the image are discussed. This proposes fixed 3 × 3 block, non-interlaced block and interlaced block schemes. A hard authenticator watermark has been proposed to tackle the problem of parity attack which is caused due to the enforcement of odd-even feature. Flippability criterion is that the number of VH, IR and C transitions remain same before and after flipping the center pixel. The example is shown as follows:



(a) (b) (c)

Fig2 (a) satisfy VH transition (b) satisfy VH and C transition (c) satisfy VH and IR transition

The embedding is done as follows:
i) Partition the image into equal size square blocks. The block size does not need to be square.
ii) Determine the flippability of the determined pixels based on the "Flippability Criterion".
iii) Once a pixel is identified as "flippable", the block is marked as "embeddable". The current "flippable" pixel is identified as the "embeddable" pixel, i.e., "embeddable" location of the block.
Proceed to the next block.
iv) Repeat steps 2 to 4 until all the blocks are processed.
v) Embed the watermark in the "embeddable" blocks by flipping the "embeddable" pixels (if needed) to enforce the odd-even feature of the number of black or white pixels in the block

Advantages

No side information is required for the watermark retrieval due to the invariant feature of the data embedding process. Different types and sizes of block can be chosen cater for different applications.

2) *Huijuan Yang and Alex C. Kot* proposed a binary image authentication technique with tampering localization by embedding Cryptographic Signature (CS) and Block Identifier. This is a two layer authentication technique as that of [5]. The overall authentication is achieved in first layer by hiding CS of image. The localization of tampering is achieved in second layer by embedding block identifier in qualified or self-detecting macro-blocks (MBs). The "flippability" of a pixel is determined by three transition criteria as in [6].
i)The given image is divided into multiple MBs and number of flippable pixels is calculated for each MB.
ii)These MBs are classified into eight categories and BI is formed.
iii)This BI is embedded on flappable pixels in each MB to enforce the odd-even feature of 3 × 3 block.
iv)The CS is embedded in those MBs containing more flappable pixels than that required to embed BIs. CS is generated by setting all the flappable locations to 0 to generate intermediate image.
v)This image is then passed to Hash() and finally by encrypting this hash value using private key CS is formed.

Advantages

The locations being tampered can be identified. It is having good visual quality.

e) Using substitution

Mrs. Gyankamal J. Chhajed and Mr. S. A. Shinde [11] proposed a method for data hiding which is based on the patterns of encrypted secret message and blocks available in image with matching pattern. Main aim is to utilize the image as much as possible with its own pattern of black and white pixels. To maintain the visual quality at most 2 pixels can be changed in the block if size is more than 2 × 2 and 1 pixel for 2 × 2 block. Embedding is done as follows:
i)Secret message is XORed using secret key.
ii) Encrypted message is matched with pattern of different block sizes starting from top, left corner.
iii) Block size is selected on the basis of match of message pattern
iv) Image is divided into selected block size and number of blocks where data is identified is identified.
v)Picture is divided into blocks of 3 × 3 from end.
vi) The information secret message + size of block + location of blocks is encrypted with secret key. Embedding of this information is done using odd-even feature.

Advantages

This method is having high hiding capacity.

f) Using run-length histogram modification

Guorong Xuan et al. [12], proposed a reversible data hiding method for binary images using run-length (RL) histogram modification. The binary image is scanned from left to right and from top to bottom to form a sequence of alternative black RL and white RL. Combining one black RL and its immediate next white RL, one RL couple is formed, thus generating a sequence of RL couples. In this scheme there is a threshold, T1, which is defined as such a sum of the black and white RLs within one RL couple that those RL couples, whose sum of black and white RLs is short than T1, will not be used for data embedding. The reason of doing so is to eliminate isolated white pixels (white RL being 1), which may defeat reversibility, i.e., the original image cannot be received exactly.

Advantages

This method can be applied to all types of binary images like text, graph, halftone, non-halftone etc. This method has good visual quality and data hiding capacity.

B *Transform domain techniques*

1) *Haiping Lu et al.* [3], proposed a DCT based data hiding technique for binary images. Watermark embedding in DC components is impossible for binary images if the embedding is done directly on binary images. This method proposes a successful watermarking algorithm for binary images, including a blurring pre-

processing and a post-embedding binarization with a biased threshold such that the watermark can survive even after binarization and offer some robustness against common processing. The embedding process is as follows:
i)The original image $f(x, y)$ is low-pass filtered using a Gaussian filter with window size of 5 × 5 and standard deviation of 1 to obtain the blurred version $f'(x, y)$.
ii) This blurred image is then split into non-overlapped blocks of 8 × 8
iii) Non-uniform 8 × 8 blocks in the original image $f(x, y)$ are i Vertical edge disappears blocks will be skipped in embedding for imperceptibility. Denote each block in $f'(x, y)$ corresponding to the non-uniform blocks in $f(x, y)$ as $f'_k(r, s)$, $r, s = 0, 1, \ldots, 7$, and $k = 0, 1, \ldots, K-1$, where K is the number of non-uniform blocks in $f(x, y)$.
iv) Each block $f_k'(r, s)$ is DCT transformed obtaining $C_k'(u,v)$.
v) The watermark is a random number sequence with Gaussian distribution $N(0,1)$. The watermark is embedded one element per block by modifying the DC value in $C_k'(u,v)$.
vi) The image block is IDCT transformed to obtain the gray level image block after embedding. This gray-level image block is then binarized to obtain the watermarked binary image block. The whole watermarked image is then obtained by replacing the K non-uniform blocks in $f(x,y)$.

Advantages:

This scheme provides good degree of robustness against common image processing.
Limitation:
This requires original image for extraction process.

2) *Haiping Lu, Alex C. Kot* and *Rahardja Susanto* proposed a binary image watermarking method through biased binarization as that of [3] but in this method DCT and IDCT are not involved which greatly simplifies watermarking. The embedding is done as follows:
i)The original image is expanded with white pixels (two at each edge) to an image of size (M+2) × (N+2).
ii)This image is then low pass filtered and blurred image is obtained by ignoring two pixels at each edge.
iii)The blurred image is then split into non-overlapped blocks of 8 × 8. Watermark is embedded by biasing the threshold in binarization.
iv)A loop is used to control the quality of watermarked image.

Advantages

This does not require original image for extraction. To improve the extraction accuracy watermark is coded in error correction code(ECC) DCT and IDCT are not involved which greatly simplifies watermarking.

3) *Huijuan Yang, Alex C. Kot, and Susanto Rahardja* , proposed a transform domain technique which hides the data orthogonally in binary image. In this, Morphological Binary Wavelet Transform (MBWT) is used. The idea in using this MBWT is to use the detail coefficients as a location map to determine the data hiding locations, since these coefficients contain the edge information in horizontal, vertical and diagonal directions. But flipping the pixels involves changing the coefficients. Flipping an edge pixel in binary images is equivalent to shifting the edge location horizontally one pixel and vertically one pixel as shown below:

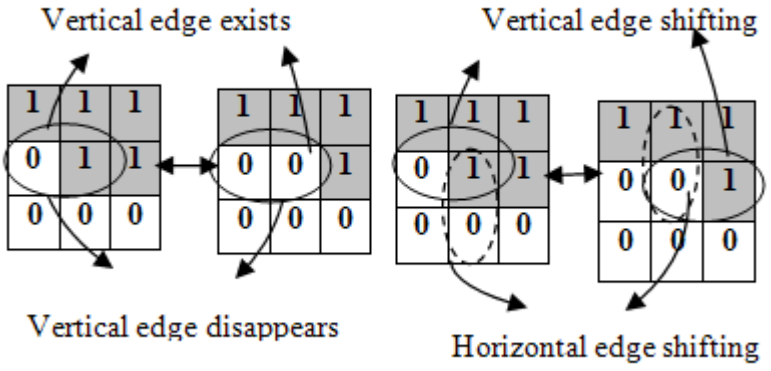


Fig 3 shifting of edges

The embedding is done as follows:
i)Compute 1-level IMBWT of Y to obtain coefficients Ck, where C represents coarse signal s, vertical detail v, horizontal detail h and diagonal detail d of Y. k represents different wavelet transforms in {ee, eo, oe, oo}.

ii) Determine the embeddability of a coarse signal based on the flipppability condition. For single processing case, a pixel is flappable if both vertical and horizontal edge exist.
iii) Hard authenticator watermark is generated and is embedded in the flippable pixels.

Advantages

This technique is having good visual quality, high embedding capacity and lower computational complexity.

IV. ANALYSIS

	Capacity	Visual quality	Robustness	Security	Computational complexity
[1]	Medium	Good	Medium	Medium	Low
[2]	Low	Good	Medium	Medium	Low
[3]	High	Good	High	High	Medium
[4]	Medium	Excellent	Medium	High	Medium
[5]	Medium	Good	Medium	Medium	Medium
[6]	Medium	Good	Medium	High	Medium
[7]	High	Good	High	High	Medium
[8]	Medium	Good	High	High	Low
[9]	High	Excellent	High	High	Low
[10]	High	Good	Medium	Medium	Medium
[11]	High	Good	Medium	Medium	Medium
[12]	High	Good	Medium	Medium	Low

V. CONCLUSION

In this paper, we have reviewed and analyzed different watermarking and steganography techniques in spatial and transform domain. We observed that watermarking techniques are more robust and secure against attacks as compared to the spatial domain techniques. Spatial domain techniques are best for some factors like visual quality. Capacity and computational complexity are common factors for both spatial and transform domain which depend on the corresponding methods.

VI. REFERENCES

[1] Q. Mei, E. K. Wong, and N. Memon, "Data hiding in binary text document," in *Proc. SPIE*, 2001, vol. 4314, pp. 369–375.
[2] Y. C.Tseng and H.-K. Pan, "Data hiding in 2-color images," *IEEE Trans. Comput.*, vol. 51, no. 7, pp. 873–878, Jul. 2002.
[3] M.Wu and B. Liu, "Data hiding in binary images for authentication and annotation", *IEEE Trans. Multimedia*, vol. 6, no. 4, pp. 528–538, Aug. 2004.
[4] H. Y. Kim and R. L. de Queiroz, "Alteration-locating authentication watermarking for binary images," in *Proc. Int. Workshop Digital Watermarking*, 2004, pp. 125–136.
[5] H. Yang and A. C. Kot, "Pattern-based data hiding for binary images authentication by connectivity-preserving", *IEEE Trans. Multimedia*, vol. 9, no. 3, pp. 475–486, Apr. 2007.
[6] Huijuan Yang and Alex C. Kot," Binary Image Authentication With Tampering Localization by Embedding Cryptographic Signature and Block Identifier*", IEEE signal processing letters, vol. 13, no. 12, december 2006*
[7] H. Lu, X. Shi, Y. Q. Shi, A. C. Kot, and L. Chen, "Watermark embedding in DC components of DCT for binary images," in *Proc., IEEE Workshop on Multimedia Signal Processing*, Dec. 9–11, 2002, pp. 300–303.
[8] Haiping Lu, Alex C. Kot , Rahardja Susanto," binary image watermarking through biased binarization"
[9] Huijuan Yang, Alex C. Kot, Susanto Rahardja,"Orthogonal data embedding for binary images in Morphological Transform domain-A high capacity approach", *IEEE transactions on multimedia, vol. 10, no. 3, april 2008*
[10] Mrs. Gyankamal J. Chhajed ,Mrs. Vandana Inamdar, Mrs Vahida Attar,"Steganography in black and white picture images", 2008 Congress on Image and Signal Processing.
[11] Mrs. Gyankamal J. Chhajed, Mr. S. A. Shinde,"Efficient embedding in B&W picture images", 978-1-4244-5265 1/10/$26.00 ©2010 IEEE
[12] Guorong Xuan, Yun Q. Shi, Peiqi Chai, Xuefeng Tong, Jianzhong Teng, Jue Li," Reversible Binary Image Data Hiding By Run-Length Histogram Modification", 978-1-4244-2175-6/08/$25.00 ©2008 IEEE.

4 STEGANOGRAPHY versus WATERMARKING IV054 STEGANOGRAPHY versus WATERMARKING Differences between steganography and watermarking are both subtle and essential. The main goal of steganography is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot detect the presence of m in d'. The main goal of watermarking is to hide a message m in some audio or video.Â Substitution in binary images. If image ci has more (less) black pixels than white pixels and mi = 1 (mi = 0), then ci is not changed; otherwise the portion of black and white pixels is changed (by making changes at those pixels that are neighbors of pixels of the opposite color). Steganography and Digital Watermarking: introduction. Steganography comes from the Greek and literally means "covered writing".[JJ98-1] It is one of various data hiding techniques, which aims at transmitting a message on a channel where some other kind of information is already being transmitted. This distinguishes steganography from covert channel techniques, which instead of trying to transmit data between two entities that were unconnected before.Â Both classical steganography and digital watermarking are based on a fundamental assumption: it is quite easy to foil the human senses.