ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A New Secure Image Transmission Approach for Videos Based On Mosaic Image and Pixel Color Transformation

Mohd Khadeer
M.Tech (VLSI System Design)
Department of Electronics Engineering
VIF College of Engineering and Technology,
Hyderabad, T.S, India.

Priyanka Thakur
Assistant Professor
Department of Electronics Engineering
VIF college of Engineering and Technology,
Hyderabad, T.S, India.

Imthiazunnisa Begum
HoD,
Department of Electronics Engineering
VIF college of Engineering and Technology,
Hyderabad, T.S, India.

Abstract:

This paper presents an approach where mosaic image generation has done by dividing the secret image in to fragments and transforming their respective color characteristics into corresponding blocks of the target frames. Usage of the pixel color transformation helps to yield the extracted secret image based on the untransformed color space values. This approach helps to eliminate the flickering artifact to achieve the lossless data recovery in motion related videos.

The methods used in it are color transformation between blocks and choosing appropriate target blocks and rotating them in concerned angle which stores the data more securely. Embedding the relevant information and creating mosaic frames from both target video and secret image then extracting the previously embedded information and hence recovering secret image. Earlier, the secret image was recovered from the target image forming secret fragment visible mosaic image but, in this project it is aimed to design the method that can transform a secret image into a secret fragment-visible mosaic frame that has the visual appearance of any selected target video without the need of a database.

Experimental results show good robust behavior against all incidental and accidental attacks and comparison to the conventional algorithms performance evaluation has been increased in a significant way. The PSNR, RMTT and the RMSE values on videos adding noise and without noise are calculated.

I. INTRODUCTION

Currently, images from various sources are frequently utilized and transmitted through internet for various applications such as, online personal photograph albums, confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Recently, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding. Image encryption is a technique that makes use of natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion and diffusion properties.

The encrypted image is a noise image so that no one can obtain the secret image from it unless he/she has

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

the correct key. However, the encrypted image is a meaningless file, which cannot provide additional information before decryption andMay arises an attacker's attention during transmission due to its randomness in form. An alternative to avoid this problem is data hiding that hides a secret message into a cover image so that no one can realize the existence of the secret data.

The proposed method is inspired by Lai and Tsai, in which a new type of computer art image, called secret-fragment-visible mosaic image, was proposed. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target video preselected from a database. But an obvious weakness of Lai and Tsai is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image. Using their method,in this project, a new technique for secure image transmission is proposed, which transforms a secret image into a meaningful mosaic frame which looks like an image. The transformation process is controlled by a secret key, and only with the key can a person recovers the secret image nearly lossless from the mosaic image, called secret-fragment-visible mosaic image, has been proposed. The mosaic frame is the result of rearrangement of the fragments of a secret image and the target video.

Figure 1: Result yielded by the proposed method. (a) Secret image. (b) Target video. (c) Secret-fragment-visible mosaic image created from (a) and (b) by the proposed method.

The above figure show a result yielded by the proposed method. Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks. Next, the color characteristic of each tile image is transformed to be that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. Relevant schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image.

II. COLOR SPACE

A device color space simply describes the range of colors, or gamut, that a camera can see, a printer can print, or a monitor can display. Editing color spaces, on the other hand, such as adobe RGB or sRGB, are device-independent. They also determine a color range you can work in. Their design allows you to edit images in a controlled, consistent manner. A device color space is tied to the idiosyncrasies of the device it describes. An editing space, on the other hand, is gray balanced — colors with equal amounts of Red, Green, and blue appear neutral. Editing spaces also are perceptually uniform; i.e. changes to lightness, hue, or saturation are applied equally to all the colors in the image.

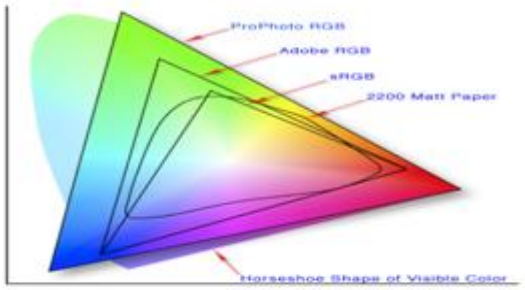


Figure 2 - A comparison of the chromaticity's enclosed by some color spaces.

Understanding the concept

A wide range of colors can be created by the primary colors of pigment (cyan (C), magenta (M), yellow (Y), and black (K)). Those colors then define a specific color space. To create a three-dimensional representation of a color space, we can assign the amount of magenta color to the representations X axis, the amount of cyan to its Y axis, and the amount of yellow to its Z axis. The resulting 3-D space provides a

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

unique position for every possible color that can be created by combining those three pigments.

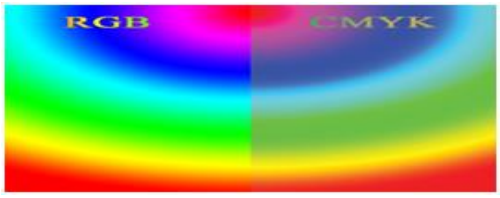


Figure 3 - A comparison of RGB and CMYK color models.

This image demonstrates the difference between how colors will look on a computer monitor (RGB) compared to how they will reproduce in a CMYK print process.

Conversion

Color space conversion is the translation of the representation of a color from one basis to another. This typically occurs in the context of converting an image that is represented in one color space to another color space, the goal being to make the translated image look as similar as possible to the original.

Color space fundamentals

Computer monitors emit color as RGB (red, green, and blue) light. Although all colors of the visible spectrum can be produced by merging red, green and blue light, monitors are capable of displaying only a limited gamut (i.e., range) of the visible spectrum. Whereas monitors emit light, inked paper absorbs or reflects specific wavelengths. Cyan, magenta and yellow pigments serve as filters, subtracting varying degrees of red, green and blue from white light to produce a selective gamut of spectral colors.

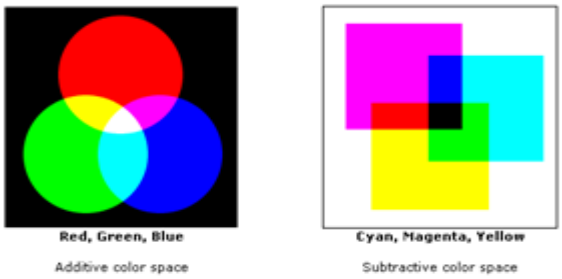


Figure 6 additive and subtractive color spaces

CMYK versus RGB color spectrum

Refer to the instructions for authors for your journal to determine if files should be supplied as RGB or CMYK. Some printers may prefer your files be delivered in RGB with ICC profiles attached, as this allows the printer to use color management methods when converting to CMYK. Other printers may prefer your files in the CMYK (Cyan/Magenta/Yellow/Black) mode, as this is the mode required for the printing process. If an RGB (Red/Green/Blue) file is submitted, it must be converted to CMYK for print.

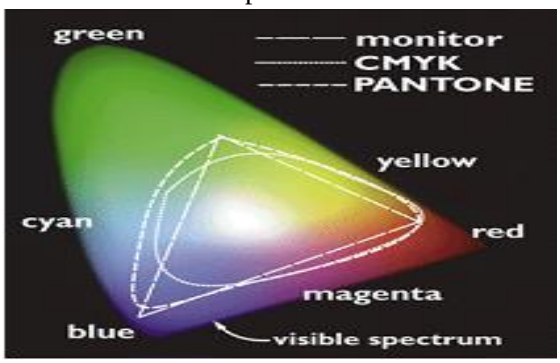


Figure 7 - RGB versus CMYK color spectrum.

Image half tones

In offset lithography, the density of CMYK inks cannot be varied in continuous fashion across an image, so a range is produced by means of half toning. In half toning, translucent CMYK ink dots of variable size are printed in overlapping grids. Grids are placed at different angles for each of the ink colors. Smaller halftone dots absorb less light; thus, as a result of an increase in the amount of reflected light, apparent density is decreased and the object appears lighter.

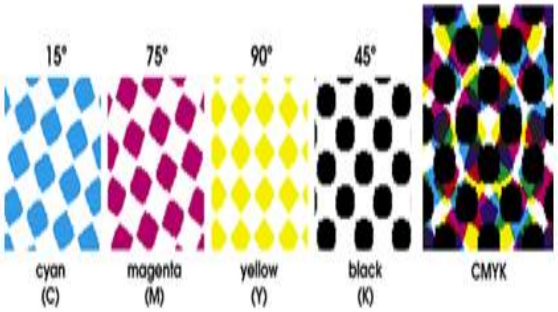


Figure 8 – Image Halftones.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

III. IDEA OF THE PROPOSED METHOD

Introduction

The proposed method includes two main phases as shown

A) Mosaic image creation and

B) Secret image recovery.

In the first phase, a mosaic image is yielded, which consists of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations.

The phase includes four stages:

1) Fitting the tile images of the secret image into the target blocks of a preselected target image;

2) Transforming the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image;

In the second phase, the embedded information is extracted to recover nearly lossless secret image from the generated mosaic image. The phase includes two stages:

1) Extracting the embedded information for secret image recovery from the mosaic image, and 2) Recovering the secret image using the extracted information.

Idea of mosaic image generation

Problems encountered in generating mosaic images are discussed in this section with solutions to them proposed.

Color transformations between Blocks

In the first phase of the proposed method, each tile image T in the given secret image is fit into a target block B ina preselected target image. Since the color characteristics of T and B are different from each other, how to change their color distributions to make them look alike is the main issue here.

More specifically, let T and B be described as two pixel sets {p1, p2, . . . ,pn} and {p_1, p_2, . . . , p_n }, respectively. Let the color of each pi be denoted by (ri, gi, bi) and that of each p_iby (r_i, g_i, b_i). At first, we compute the means and standard deviations of T and B, respectively, in each of the three color channels R, G, and B by the following formulas:

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i, \quad \mu_c' = \frac{1}{n}\sum_{i=1}^{n} c_i' \qquad (1)$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2}, \quad \sigma_c' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i' - \mu_c')^2} \qquad (2)$$

In which ci and ci′denote the C-channel values of pixels pi and p_i, respectively, with c = r, g, or b and C=R, G, or B. Next, we compute new color values (r__i,g__i, b__i) for each pi in T by

$$c_i'' = q_c(c_i - \mu_c) + \mu_c', \qquad (3)$$

in which qc = σ c′/σcis the standard deviation quotient and c = r, g, or b. It can be verified easily that the new color mean and variance of the resulting tile image T′ are equal to those of B, respectively. To compute the original color values (ri, gi, bi) of pi from the new ones (r__i,g__i, b__i), we use the following formula which is the inverse of (3):

$$c_i = (1/q_c)(c_i'' - \mu_c') + \mu_c. \qquad (4)$$

Furthermore, we have to embed into the created mosaic image sufficient information about the new tile image Tforuse in the later stage of recovering the original secret image. Choosing appropriate target blocks and rotating blocks to fit better with smaller RMSE value

In transforming the color characteristic of a tile image T to be that of a corresponding target block B as described above, how to choose an appropriate B for each T is an issue. For this, we use the standard deviation of the colors in the block as a measure to select the most similar B for each T.

Handling overflows/underflows in color transformation

After the color transformation process is conducted as described previously, some pixel values in the new tile imageT′might have overflows or underflows. To deal with this problem, we convert such values to be non-

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

overflow or non-under flow ones and record the value differences as residuals for use in later recovery. Specifically, we convert all the transformed pixel values in T′not smaller than 255 to be 255, and all those not larger than 0 to be 0.

Embedding information for secret image recovery

In order to recover the secret image from the mosaic image, we have to embed relevant recovery information into the mosaic image. For this, we adopt a technique proposed by Coltuc and Chasseryand apply it to the least significant bits of the pixels in the created mosaic image to conduct data embedding. Unlike the classical LSB replacement methods, which substitute LSBs with message bits directly, the reversible contrast mapping method applies simple integer transformations to pairs of pixel values.

$$x' = 2x - y, \quad y' = 2y - x$$

$$x = \left\lfloor \frac{2}{3}x' + \frac{1}{3}y' \right\rfloor, \quad y = \left\lfloor \frac{1}{3}x' + \frac{2}{3}y' \right\rfloor. \qquad (6)$$

These data items for recovering a tile image T are integrated as a five-component bit stream of the form M = t1t2. . .tmr1r2… m1m2. . .m48q1q2. . .q21d1d2. . .dkin which the bit segments t1t2 . . . tm, r1r2, m1m2 . . . m48, q1q2. . . q21, and d1d2 . . . dkrepresent the values of the index of B, the rotation angle of T, the means of T and B, the standard deviation quotients, and the residuals, respectively.

1) The index of B needs m bits to represent, with m computed by

$$m = \lceil \log[(W_S \times H_S)/N_T] \rceil \qquad (7)$$

IV. EXISTING METHODS

Introduction

Image encryption is a technique that makes use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion and diffusion properties. The encrypted image is a noise image so that no one can obtain the secret image from it unless he/she has the correct key.

Secure image transmission

Steganography is the art and science of invisible communication. This can be achieved by hiding the information into the original information. The word steganography is derived from the greek words "stegos" meaning "cover" and "graphia" which means "writing". In most of the image processing applications, steganography is used to hide the information in the images.

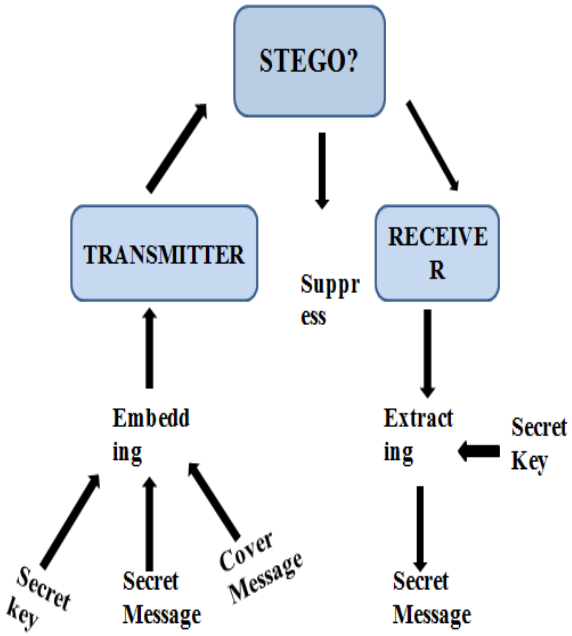


Figure 9- Basic Steganography System Scenario

Conventional methods

In the image-processing applications, the conventional methods that are most frequently used are cryptography, watermarking and steganography using Least- Significant Bit (LSB) algorithm.

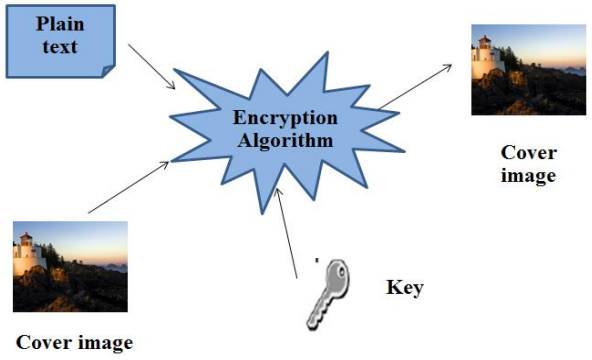


Figure 10(a) - Encryption Process

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

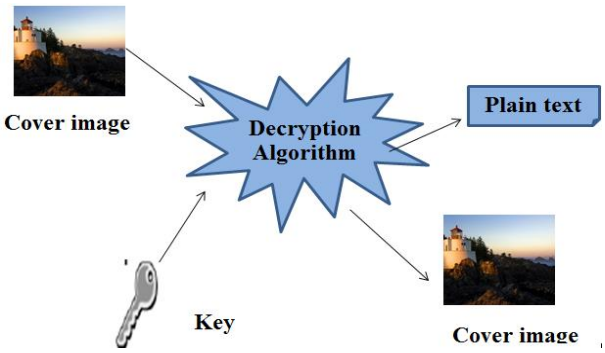


Figure 10 (b) - Decryption Process

These two methods protect information from the unwanted parties and security attacks.

Water-marking technique enables the intellectual property of the owner to identify the customers who break their licensing agreement by supplying the property to third parties. Fig 10(a) and 10(b) represents the encryption and decryption processes in cryptography.

End

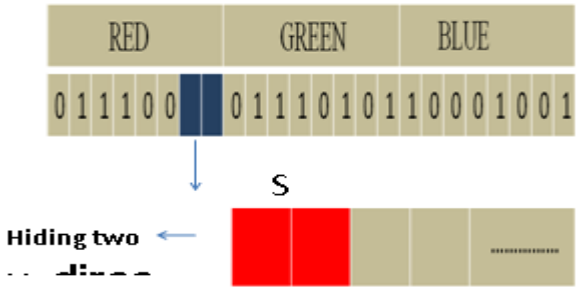


Figure 11(a): Hiding by using least significant method

The images are mainly divided into three types. They are:

•Binary (Black-White)

•Gray-scale

•Red-Green-Blue Image.

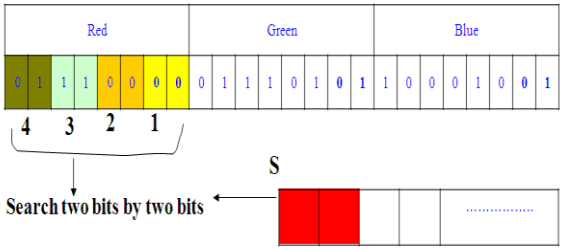


Figure 11(b) - Steganography using RGB

Decomposition

The RGB method is the most significant and is proved to be efficient as it contains a lot of information that helps in hiding the secret information with a bit change in the Image resolution. It improves the image quality and makes the message more secure. This method uses the RGB image as the carrier and the least- Significant Bits (LSB) to hide the secret message. The images below Fig(a) and Fig(b) below show the carrier(cover) image and the secret image.

Figure 12(a): Original Image (cover image)

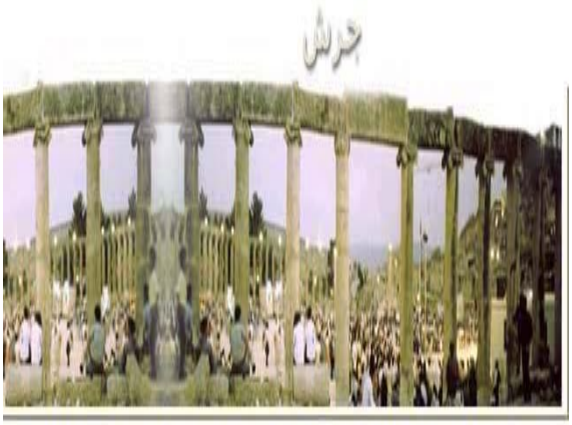


Figure 12(b): Secret image

Disadvantages of existing system:

A main issue of the methods for hiding data in images is the difficulty to embed a large amount of message data into a single image. Most image compression methods, such as JPEGcompression, are not suitable for line drawings and textual graphics, in which sharp contrasts between adjacent pixels are often destructed to become noticeable artifacts.

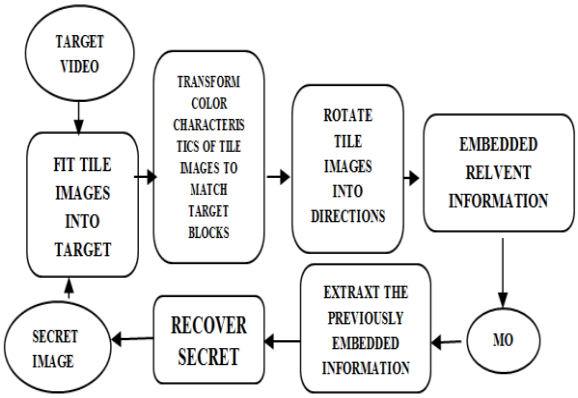
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

V. PROPOSED SYSTEM

Introduction

In this Project, a new technique for secure image transmission is proposed, which transforms a secret image into a meaningful mosaic frame which looks like an image.

Block diagram



Architecture

Color transformations between blocks

In the initial part of the planned technique, every tile image T within the given secret image is match into a target block B in a preselected target frame. Since the color characteristics of T and B are totally different from one another, the way to amendment their color distributions to form them look alike is that the main issue here color transfer theme in this face t, that converts the color characteristic of an image to be that of another within the l αβ color area.

More specifically, let and B be described as 2 pixel sets{p1,p2 ,p3,……..p_n}and{p_1^',p_2^' ……p_n^'} Severally. Let the color of every pi be denoted by ((r_i,g_(i,) b_i). which of everyp_1^' by (r_i^',g_(i,)^' b_i^'). At first, we tend to work out the means and standard deviations of T and B, severally; in every of the 3 color channels R, G, and B by the subsequent formulas:

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i, \quad \mu_c' = \frac{1}{n}\sum_{i=1}^{n} c_i' \qquad \text{——————} (1)$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i - \mu_c)^2}, \quad \sigma_c' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i' - \mu_c')^2} \qquad \text{——————} (2)$$

In which〖 c〗_i andc_i^',denote the C-channel values of pixels p_i andp_i^', severally, with and C=R,G,or B. Next, we have a tendency to compute new color values (r_i^',g_(i,)^' b_i^') for each p_i in T by

$$c_i'' = q_c(c_i - \mu_c) + \mu_c', \qquad \text{——————} (3)$$

Inq_c=σ_c/σ_c^' is the standard deviation quotient and c=(r,g,orb). It can be verified easily that the new color mean and variance of the resulting tile image T_^'are equal to those of B, respectively. To compute the original color values ((r_i,g_(i,) b_i) of p_i from the new ones (r_i^',g_(i,)^' b_i^'), we use the following formula which is the inverse of (3)

$$c_i = (1/q_c)(c_i'' - \mu_c') + \mu_c. \qquad \text{——————} (4)$$

Furthermore, we've to embed into the created mosaic image sufficient data concerning the new tile image T_h^'foruse within the later stage of convalescent the initial secret image. For this, theoretically we will use (4) to compute the initial pixel price of p_i However, the concerned mean and normal deviation values within the formula area unit all real numbers, and it is impractical to embed real numbers, every with several digits, in the generated mosaic image. Therefore, we limit the numbers of bits wont to represent relevant parameter values in (3) and(4).

Choosing appropriate target blocks and rotating blocks to fit better with smaller RMSE value

In transforming the color characteristic of a tile image T to be that of a corresponding target block Bas represented higher than, how to choose an appropriate B for every T is a problem. For this, we use the standard deviation of the colors within the block as a live to pick out the foremost similar for each T.

Handling overflows/underflows in color transformation

After the color transformation process is conducted as described previously, some pixel values in the new tile imageTmight have overflows or underflows. To deal with this problem, we convert such values to be non-overflow or non-under flow ones and record the value

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

differences as residuals for use in later recovery. Specifically, we convert all the transformed pixel values in Tnot smaller than 255 to be 255, and all those not larger than 0 to be 0.

$$c_S = \lceil 1(/q_c)(255 - \mu_c') + \mu_c \rceil ; \quad c_L = \lfloor (1/q_c)(0 - \mu_c') + \mu_c \rfloor . \qquad (5)$$

Next, for an untransformed value ci which yields an overflow after the color transformation, we compute it's residual as |ci - cS|; and for ci which yields an underflow; we compute it's residual as |cL- ci|. Then, the possible values of the residuals of ci will all lie in the range of 0 to 255 as can be verified. Consequently, we can simply record each of them with 8-bits.

Applications

Data hiding is an important role in the security of documents and images in present age to avoid illegal attackers or hackers in accessing the data. Below are some of the applications where data hiding is used.

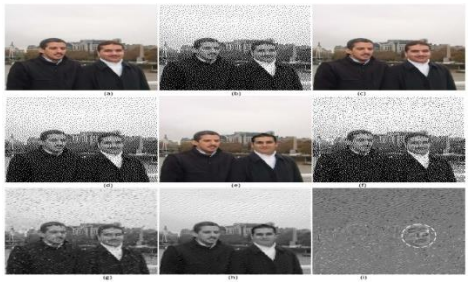


Figure 14Performance of self-embedding algorithm on securing digital data.

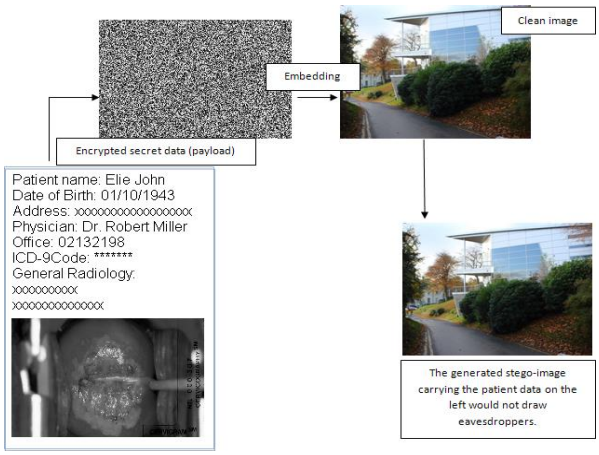


Figure 15 EPRs data being concealed in an innocuous file for secure transmission.

Image encryption

The information security is used from old ages, different person using different technique to secure their data. Following are some techniques that uses for security of images from ancient age to till date

A. steganography
B. watermarking technique
C. visual cryptography
D. without sharing keys techniques

Watermarking technique

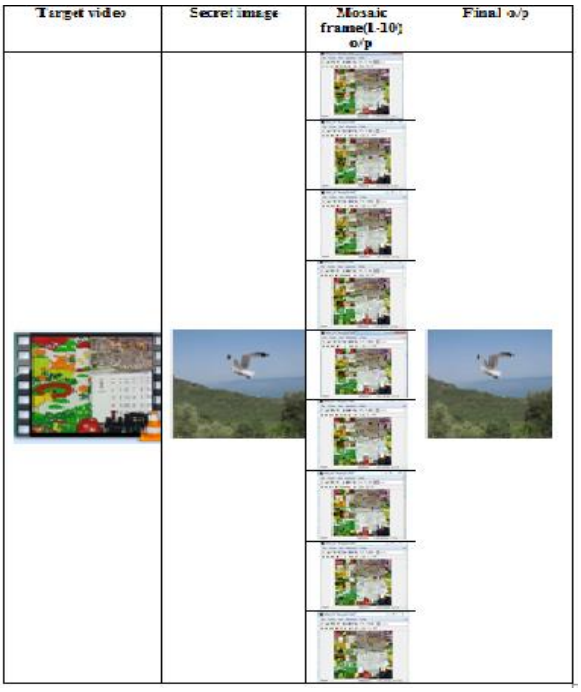
Watermarkingisalsooneofthetechniqueusedtohidethedigitalimage, digital watermarking is a process of embedding (hiding) marks which are typically invisible and that can be extracted only by owners of the authentication. This is the technology which is used with the image that cannot be misused by any other unauthorized miss users.

VI. SIMULATION AND RESULTS

Introduction

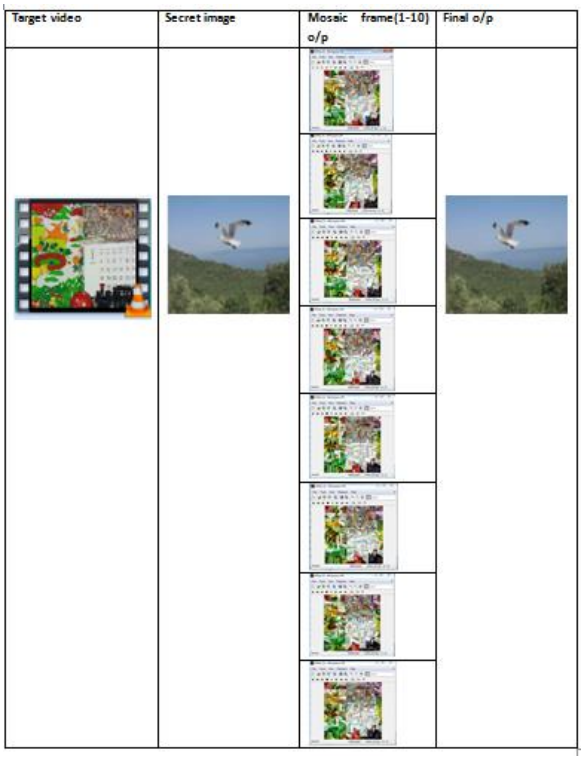
The target video and the secret image are taken as input to the formation of visible mosaic frame and final result of the image is shown below.

Without Noise



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

With Noise



Performance evaluation

Introduction

In this chapter, the tables and graphs shows the comparison values of PSNR with and without Noise,RMSE with and without noise and RMTT with and without noise.

PSNR

Frame	Without Noise	With Noise
1	38.9445	38.1707
2	38.6962	37.6823
3	39.0986	37.3891
4	38.9019	37.1343
5	38.8331	37.7797
6	39.1055	36.9046
7	38.8623	38.3832
8	38.7094	36.9742
9	39.2179	36.3426
10	38.7460	37.3649

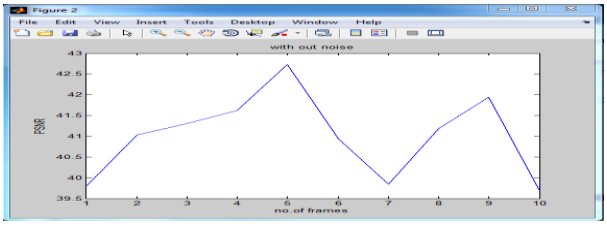
RMSE

Frame	Without Noise	With Noise
1	3.1366	3.2732
2	3.2366	3.3851
3	3.0250	3.5313
4	3.1463	3.6123
5	3.1585	3.4292
6	3.0118	3.7760
7	3.1024	3.0989
8	3.1548	3.6814
9	2.9297	3.9250
10	3.1263	3.4870

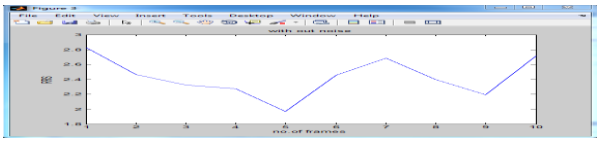
RMTT

Frame	Without Noise	With Noise
1	48.3478	56.4944
2	48.1383	57.5694
3	47.4585	56.5174
4	47.6130	58.1523
5	47.5795	56.4795
6	46.6814	58.0026
7	47.2583	58.4653
8	47.1895	57.1809
9	47.5983	58.8408
10	47.7543	57.8393

Without Noise Graphs

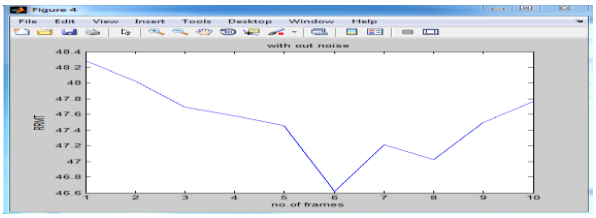


(a) PSNR Graph



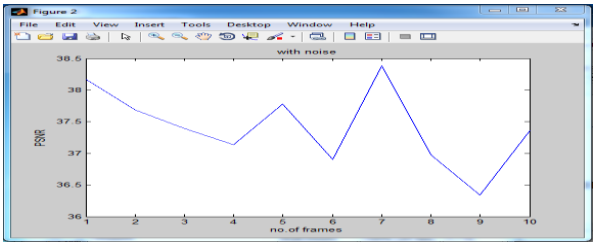
(b) RMSE Graph

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

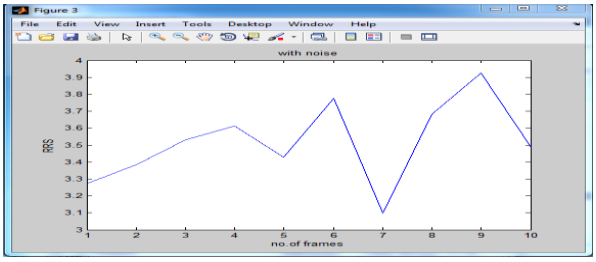


(c) RMTT

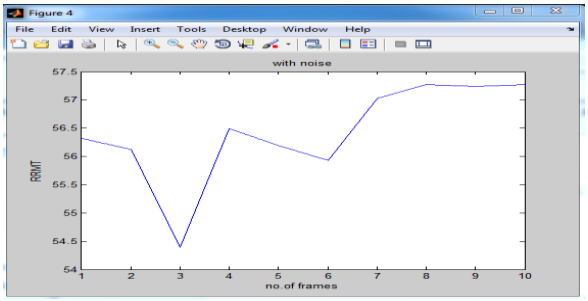
WithNoise Graphs



(d) PSNR Graph



(e) RMSE Graph



(f) RMTT Graph

The numerical values and graphs are shown and the values are differing since the noise is added. The distorted values have been calculated.

The average value of PSNR without Noise =38.91
The average value of PSNR with Noise=37.41
The average value of RMSE without Noise=3.1027
The average value of RMSE with Noise=3.51
The average value of RMTT without Noise=47.56
The average value of RMSE with Noise=46.09

VII. CONCLUSION

A new secure image transmission method has been proposed, which not only can create meaningful mosaic images but also can transform a secret image into a mosaic frames. By the use of proper pixel color transformations as well as a skillful scheme for handling overflows and underflows in the converted values of the pixels' colors, secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target video. Also, the original secret images can be recovered nearly lossless from the created mosaic images. Good experimental results have shown the feasibility of the proposed method.

In future, secure image transmission plays vital role in all prominent areas such as military, medicine, video application. So this can be improved in near future for better security.

REFERENCES

1. J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurcat. Chaos, vol. 8, no. 6, pp. 1259–1284, 1998.

2. G. Chen,Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solit. Fract., vol. 21, no. 3, pp. 749–761, 2004.

3. L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," Chaos Solit. Fract., vol. 24, no. 3, pp. 759–765, 2005.

4. H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," Chaos Solit.Fract., vol. 32, no. 4, pp. 1518–1529, 2007.

5. S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos Solit.Fract., vol. 35, no. 2, pp. 408–419, 2008.

6. D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaosbased image encryption

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

algorithm," Chaos Solit. Fract., vol. 40, no. 5, pp. 2191–2199, 2009.

7. V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption," Opt. Commun., vol. 284, no. 19, pp. 4331–4339, 2011.