



Information hiding method based on Steganography and Image morphing

¹Bhushan Zope,²Soniya Patil

¹Assistant Professor,²Research Scholar

Computer Department

Pune Institute of Computer technology, University

Pune, Maharashtra

India

Abstract: *Steganography is used to hide the information inside the cover image. Cover- rate will be increased if the cover is similar to secret as there will be less data to hide. We can generate similar images with the Image Morphing technique. So here new data hiding technique is proposed based on Image Morphing and Steganography. The intermediate images generated in the morphing process are very much similar to both source and destination image. So if we use one of such intermediate image as the secret image and destination image as cover image, then by using steganography we can hide more data using same cover image. With the help of experimental results we have showed that data embedding intensity is increased to many folds over old steganographic methods. The proposed system embeds information with intensity equals to 1 and with higher imperceptibility and security.*

Keywords: Image Representation – Morphological, image processing and computer vision, Steganography.

I. Introduction

In recent time the use of digital media is increased in many folds. With increase in popularity of digital media, security related issues of digital media have gain importance. Confidentiality is the one of such issue. To make the digital media more confidential we can use the cryptography and steganography. The main problem with cryptography is that, it reveals the existence of important data. If encrypted Message is caught by intruder then even if he can't understand the confidential data, he can gain the knowledge of certain secret communication between two parties. Also because of this knowledge, cipher text attracts the interest of cryptanalysts. In many system, revelation of existence of secret message leads to failure of that system. Because of this drawback, steganography has gained importance in recent time. The word Steganography is derived from the Greek words Steganos meaning "covered" and graphy meaning "writing or drawing" i.e. concealed writing. Wikipedia defines Steganography as the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Christian chachin [7] defines steganography as the art and science of communicating in such a way that the presence of a message cannot be detected. In steganography important information (secret) is hidden in the innocent looking data (cover).

Steganography is being used from ancient ages. One of the earliest methods is tattooing a message on a slave's head. When their hair grew back, the messenger was sent to their destination. There are many examples in history where Steganography was used in the war times. The study of steganography can be traced to [8], in which the *Prisoners' Problem* was proposed. The scenario explained there is: Alice and Bob were in jail, and they wanted to make a escape plan. However, warden, Willie strictly observes all their communications. Willie would put them into solitary confinement if he detects any encrypted messages. Therefore, Alice and Bob must find a way to transfer their secret using innocent looking cover text.

Image morphing is also known as image metamorphosis, which is also a Greek word which means transformation. Thus image morphing is process in which one image is changed into other image through seamless transition. This seamless transition is achieved by generating series of intermediate images. It is often used to create the special effects in movies such as Terminator, Willow and Indiana Jones and the last crusade, in music videos such as Michael Jackson's Black or White [10]. Morphing is also used in the gaming industry to add engaging animation to video games and computer games. However, morphing techniques are not limited only to entertainment purposes. Morphing is a powerful tool that can enhance many multimedia projects such as presentations, education, electronic book illustrations, and computer-based training. Morphing process between two images is initiated with the specification of the correspondence points. This phase is usually called as 'feature specification'. The feature specification process defines the corresponding feature primitives for both

images. This process is the most tedious aspect of morphing and performed manually in most cases. Each primitive denotes the image landmark or feature.

Corresponding feature sets are then used to compute the mapping function, which is called as 'warp function'. This warp function calculates and transforms each pixel in one image to new position in other image. Thus it specifies the relation between pixels in both images. This brings the last phase of morphing: transition control. Transition control blends in the color between both images and also decides the rate of warping [9]. Transition control is responsible of smooth and fluid transformation of images. Thus morphing is a three phase method viz. Feature specification, warp generation, and transition control.

This paper has been organized as following sections:- Section II contains the literature review of steganography and image morphing. Section III describes the proposed model with system diagram. Mathematical Modeling of the process has been discussed in Section III. Section IV describes experimental setup while its results are shown and discussion is done in Section V. Section VI draws the conclusion and states the future work.

II. LITERATURE REVIEW/ MOTIVATION

Steganography is the hiding of information in innocent looking cover. The type of cover determines the type of steganography. various type of steganography systems are shown in fig.1.

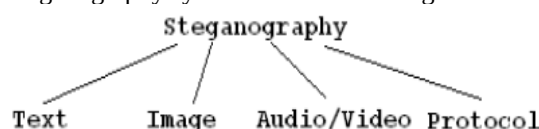


Figure 1

Our focus in this work is on image based steganography. In digital images, information can be hidden into various domains. One can hide the data by altering the least important bits of the cover image. Such type of steganography is called as Spatial Domain steganography. Various algorithms such as LSB, Modulus Arithmetic, Adjacent Pixel Difference, and Histogram shifting methods are developed under spatial domain. While methods such as DCT based methods, wavelet transform methods, frequency transform methods are come under another type of steganography, called as transform domain steganography. Abbas Cheddad, JoanCondell, KevinCurran and PaulMcKevitt [2] extensively review the various steganography techniques.

Image morphing has three main steps viz. feature extraction, warp generation and color transition. There are many algorithms present for each step. The basic image morphing method is Cross-Dissolve, which is very simple and easy method but it is not that effective. Other notable morphing methods are Mesh Warping[10],triangular mesh warping[11],field morphing[12], Scattered Data Interpolation[13], Energy Minimization[14], Multilevel Free-Form Deformation[15]. The survey of all such methods is done by George Wolberg in [9].

The use of image morphing for information hiding is proposed by Hiroyuki Nakamura and Qiangfu Zhao in their work [4]. In [4], authors proposed that the intermediate images generated in morphing process can be used as stego data to hide the source and destination images. They considered secret image as source image and cover image as destination image, in morphing process. Also both the source image and the target image can be hidden in the intermediate image. To ensure the security, the cover image is used as one of the stego keys, and is kept secretly.

In this paper we proposed the new method for image security based on morphing and steganography.

MOTIVATION:

The main motivation for this work is the fact that if secret to be embedded and the cover are similar to each other then we have to hide only the information which is different than cover.

III. Proposed System

A. Design concept

Our technique is based on image morphing and steganography. The intermediate images generated in image morphing are similar to source image and destination image. First image in the sequence is very similar to source image while last image is similar to destination image. As we move from first image to last image the similarity with source image decreases while destination image increases. We can select one of such intermediate image as secret image and destination image as cover image. Both these images have strong correlation between each other. So information contained in both images is similar. So we have to hide only information which is different from cover image. Thus using steganography techniques on these both images we can achieve more hiding capacity.

Figure2 describes the block diagram of proposed model. In the proposed system, both secret image and cover images are morphed using available morphing techniques and numbers of intermediate images are generated.

Then one of the images out of them is selected using standard deviation as a selection criterion. The selected image is then becomes the new secret image for the steganography process. Then using cover image and new secret image and using any existing steganography process, stego data is produced, which can be sent across the public network. Once receiving the stego data at other end, the secret image is extracted using extraction techniques. This extracted secret image is the intermediate image generated in morphing technique. The actual secret image can be obtained by de-morphing the extracted image with the help of morphing keys.

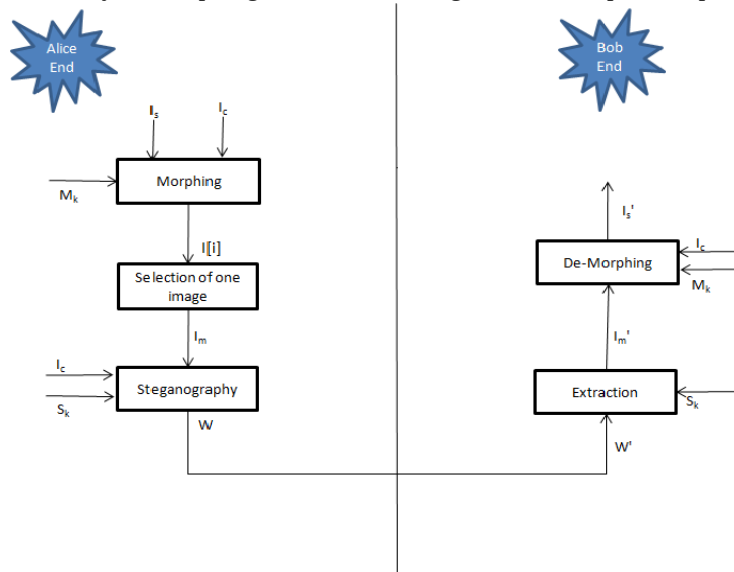


Figure 2

B. Model for proposed system

System set S can be defined as: $S = \{I_s, I_d, I^Q, I_w, K, I_s'\}$

Where

I_s : Secret Image/ Source, $\{s_1, s_2, \dots, s_n\}$, i.e. Each image in system is treated as the array of N pixel;

I_d : Destination Image/ cover image = $\{d_1, d_2, \dots, d_n\}$.

I^Q : Set of Intermediate images = $\{I_1, I_2, I_3, \dots, I_r\}$

Where $I_i = \{i_1, i_2, i_3, \dots, i_n\}$;

I_w : stego-image = $\{w_1, w_2, \dots, w_n\}$.

K : keys = $\{S_k, M_k\}$

Where

S_k : stego-keys = $\{I_d, b_n, \min\}$;

M_k : morph-keys = $\{I_d, N, r\}$;

There are 5 important modules in the system.

1. Morphing:

Morphing function can be defined as:

$M_v: (I_s, I_d, M_k) \longrightarrow I^Q$

Where Function M_v takes the I_s , I_d and M_k as input and generates the N intermediate images, where $N \in M_k$.

Every pixel in intermediate image I_j can be generated as:

$$I_j = (1-j/N) I_s + (j/N) I_d$$

Thus

$$I_0 = I_s \text{ and } I_N = I_d,$$

2. Intermediate images selection:

$F: I^Q \longrightarrow I_r$

Function F selects the one image out of N images generated in first stage, which will be more suitable for steganography.

The selection will take place according to following criteria:

Select image I_r such that

Minimize: Standard deviation, $\sigma(I_r, I_d)$

Subject to: $PSNR(I_m(r), I_d) > 36$

Where $I_m(r)$ is stegodata produced with help of I_r

Usually, people cannot feel the difference in the images if $PSNR > 36$ dB [16]. Standard deviation can be calculated using:

$$\sigma(X, Y) = \sqrt{\frac{1}{n} \sum_{i=1}^n (X(i, j) - Y(i, j))^2}$$

PSNR is calculated using:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

Where,

$$MSE = \frac{1}{n} \sum_{i=1}^n (X_i - X_i')^2$$

3. Steganography:

SK: $(I_s, I_d, S_k) \rightarrow I_w$

Function SK takes I_s, I_d, S_k as input and using steganography technique generates stego-image I_w .

For embedding process, we define

D' : Difference set,

$D' = I_r - I_d$

$D = D' - \min(D')$

I_w can be generated as:

$I_w = I_d \oplus D$

Where $\oplus$ operator that replaces last b_n bit of I_d with D .

4. Secret Extraction:

SK': $(I_w, S_k) \rightarrow I_r$

Function SK takes I_w, S_k as input and with the help of S_k , it extracts the information (secret image) I_r from stego data I_w .

For Extraction:

$D = SK'(I_w)$

• Where SK' returns the last b_n bit from I_w

$D' = D + \min(D)$

$I_r = I_d + D'$

5. Demorphing:

$M_v': (I_r, M_k) \rightarrow I_s$

Function M_v' takes I_r, M_k as input and with the help of M_k demorph the image I_r to generate secret image I_s .

Function M_v' generates the I_s with following formula:

C. Algorithms:

Algorithms explained here are combination of cross-dissolve and LSB technique.

Embedding Algorithm
Input: (I_s, I_d, S_k, M_k) Output: I_w
1. Take secret and cover image from user along with keys. 2. For each intermediate image I_i - For each pixel in I_i $I_j = (1-j/N) I_r + (j/N) I_d$ 3. For each intermediate image I_j a. Calculate $\sigma(I_j, I_d)$ b. Calculate difference set $D' = I_j - I_d$ c. Find out minimum difference from D' d. Calculate $D = D' - \min$ e. Find out maximum bit(b_n) required to represent D f. Replace b_n bit of I_d with D to get I_{jw} g. Calculate $PSNR(I_{jw}, I_d)$ 4. Select I_j such that, $\sigma(I_j, I_d)$ is minimum and $PSNR(I_{jw}, I_d) > 36$ 5. Stego-data $I_w = I_{jw}$ 6. end

Extraction Algorithm
Input: (I_w, I_d, S_k, M_k) Output: I_s
1. Take b_n LSB of I_w to get D 2. Calculate difference set $D' = D + \min$ 3. Calculate $I_r = I_d + D'$ 4. For each pixel i in I_r $I_s = (I_r - \frac{r}{N} I_d) / (1 - \frac{r}{N})$ 5. End

IV. Experimental Setup

For experimentation purpose we have used the dataset extracted from image database [18]. We have collected around 60 images from database. All the images we have considered are grayscale and 512X512 in size. We can use any size, any color model image for the dissertation but for the experimental point of view we have narrowed down our scope to above said category. Also we can combine any of the morphing and steganography

technique to verify the concept. Here as explained in section III.B, we have used cross dissolve as the morphing method and LSB as the steganography technique. We have tested the concept using cross dissolve and modulus arithmetic as well.

V. Results and discussion

1. Relation between Standard deviation and number of images generated.

Figure3 shows the relation between number of images generated and standard deviation between image selected in 2 module and destination images.

From this figure we can conclude that the minimum standard deviation between intermediate image and destination image decreases rapidly with increase in number of images generated but it becomes almost constant after 200 images. So we have to generate the minimum 200 images to get the best result.

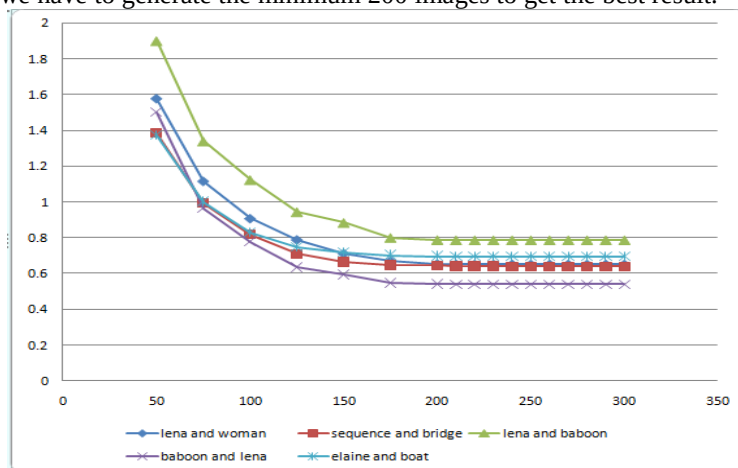


Figure 3

2. LSB Vs. Proposed method

Figure 4 shows the relation between PSNR and the number of bits used in LSB technique. The imperceptibility criteria i.e. if PSNR between two images is less than 36 then the difference between two images are imperceptible to human eye, is not fulfilled with the 4 bit and above LSB method. So maximum 3 bits/pixel are available for hiding secret. Thus using LSB technique one needs the cover of sizes 8/3 times size of secret image. Thus the embedding intensity is 3/8. Figure 5 shows the results of proposed system, where cross dissolve is used as the morphing technique and LSB as steganography technique. Both the secret and cover images are of the same size 512X512. Thus we manage to hide the secret image in cover image with same size. Hence the embedding intensity becomes 1. Also the PSNR between stego image and cover image is better than normal LSB method.

3. Modulus Arithmetic Vs. Proposed method

From the figure 6 it can be concluded that we can use maximum of modulo8 since every other number greater than 8 does not satisfy the imperceptibility criteria. So using this method we can hide 3 bits/pixel. Thus embedding intensity for this technique is also 3/8. When this technique is combined with cross dissolve we got the results, as shown in figure7. Here as well, we managed to hide the secret in same size cover image which makes embedding intensity as 1.

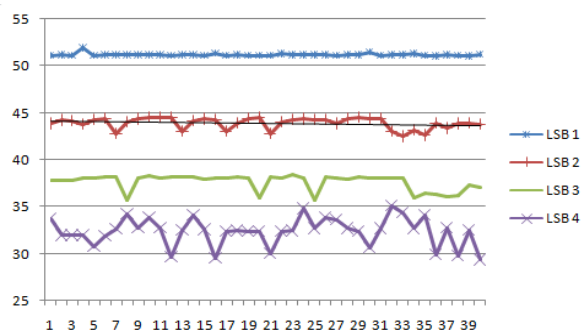


Figure 4

	Secret Image	Cover Image	PSNR
1	Sequence	Baboon	46.2275529
2	Baboon	Sequence	44.03472305
3	Baboon	Women	46.46520675
4	Boat	Bridge	46.59634429
5	Bridge	Baboon	46.28391442
6	Bridge	Sequence	46.4383638
7	Bridge	Women	46.4432361
8	Elaine	Sequence	46.41502132
9	Elaine	Bridge	46.52786314
10	Sequence	Boat	51.16252778

Figure 5

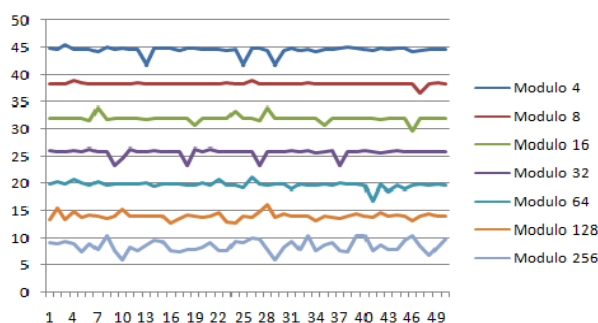


Figure 6

	Secret Image	Cover Image	PSNR
1	Women	Lena	46.29895914
2	Baboon	Boat	44.06351293
3	Lena	Sequence	44.78037224
4	Bridge	Sequence	46.4383638
5	Baboon	Lena	51.01498888
6	Elaine	Bridge	46.52786314
7	Sequence	Baboon	46.2275529
8	Elaine	Baboon	46.24674916
9	Women	Boat	44.77486089
10	Sequence	Women	46.46992844

Figure 7

4. Effect on Security

In normal LSB method when last bits of stego image are extracted, they reveal the secret directly. So very basic step in steganalysis is to extract last bits of image and to see whether it gives any secret or not. But in proposed method, even if last bits are extracted, they don't reveal anything about secret. In order to extract secret out of last extracted bits one must know the procedure and must have the morph and stego keys. Thus the overall security of method is increased.

VI. Future Work

The basic assumption of any steganography technique is that the stego keys are known to both the communication parties. In proposed technique as well, we have assumed that both morph and stego keys are known to both ends. But various ways to distribute the keys in secure and secret manner needs to be researched. Also PSNR between stego image and cover image from the above proposed method is very high so there is scope of embedding more secret in that stego image. So we can use the proposed method for multi level embedding which will give even higher embedding intensity. But this concept needs to be verified.

VII. Conclusion

This paper presents a new information hiding technique, on the base of image morphing and steganography. It uses one of intermediate image generated with morphing technique, as the secret image and destination image as cover image. We have shown the results with cross dissolve-LSB and cross dissolve-modulus arithmetic methods however any other combination of morphing-steganography technique can be used. The result shows that the embedding intensity had increased tremendously while the imperceptibility is also higher. This technique also provides more security than original techniques.

VIII. References

- [1] Tseng, Y.-chee, Chen, Y.-yuan, & Pan, H.-kuang, "A Secure Data Hiding Scheme for Binary Images," IEEE transactions on communications, vol. 50(8), pp. 1227-1231, 2002.
- [2] Abbas Cheddad, JoanCondell, KevinCurran, PaulMcKevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, Vol. 90(3), pp.727-752, 2010.
- [3] H.B.Kekre,A.A. Athawale, & U.A. Athawale," Increased Capacity for Information Hiding using Walsh Transform," International Conference and Workshop on Emerging Trends in Technology (Icwet), pp. 96-101, 2010.
- [4] H. Nakamura, & Q. Zhao," Information Hiding Based on Image Morphing," 22nd International Conference on Advanced Information Networking and Applications, pp.1585-1590, 2008.
- [5] Hong, W., Chen, T.-shou, & Shiu, C.-wei," Reversible Data Hiding Based on Histogram Shifting of Prediction Errors," International Symposium on Intelligent Information Technology Application Workshops, pp. 292-295, 2008.
- [6] XIE Qing, XIE Jianquan, XIAO Yunhua, "A High Capacity Information Hiding Algorithm In Color Image," e-business and information system security, pp. 1-4, 2010.
- [7] Christian Cachin, "An information-theoretic model for steganography," *Information and Computation*, vol.192(1), pp.41-56, 2004.
- [8] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Proc. CRYPTO '83*, pp. 51-67,1983.
- [9] G. Wolberg, "Recent advances in image morphing,"*Proceedings of CG International '96*, pp. 64-71, 1996.
- [10] G.Wolberg. *Digital ImageWarping*.IEEE Computer Society Press, Los Alamitos, CA, 1990.
- [11] J. Ruppert, "A Delaunay Refinement Algorithm for Quality 2-Dimensional Mesh Generation", presented at J. Algorithms, pp.548-585, 1995.
- [12] T. Beier and S. Neely, "Feature-based image metamorphosis," *Proc. Computer Graphics*, vol. 26(2), pp. 35-42, 1992.
- [13] N. Arad, N. Dyn, D. Reissfeld, and Y. Yeshurun, "Image warping by radial basis functions: Applications to facial expressions," *CVGIP: Graphical Models and Image Processing*, vol. 56(2), pp. 161-172, 1994.
- [14] S.-Y. Lee, K.-Y.Chwa, J. Hahn, and S. Y. Shin., "Image Morphing Using Deformation Techniques," *The Journal of Visualization and Computer Animation*, vol. 7(1), pp. 3-23, 1996.
- [15] S.-Y. Lee, K.-Y.Chwa, S. Y. Shin, and G. Wolberg, "Image metamorphosis using snakes and free-form deformations," *Computer Graphics (Proc. SIGGRAPH '95)*, pp. 439-448, 1995.
- [16] Peng, Hong and Lin, YanBin and Wang, Yuanzhi" An Information Hiding Algorithm Based on Blocks and Scrambling," *JCAI*, IEEE Computer Society, pp. 327-329, 2009.
- [17] Sayuthi Jaafar, Azizah A Manaf, Akram M Zeki "Steganography Technique Using Modulus Arithmetic," 9th International Symposium on Signal Processing and Its Applications, 2007. ISSPA 2007.
- [18] USC-SIPI image database,<http://sipi.usc.edu/services/database/Database.html>