Multimed Tools Appl
DOI 10.1007/s11042-013-1708-1

A steganographic method via various animations in PowerPoint files

Wen-Chao Yang · Ling-Hwei Chen

Abstract In a PowerPoint file, animation effects are used to emphasize objects, timing effects are used to control the presentation time, and slide transition effects are used to highlight particular slides. Thus, using various effects can make the presentation of a PowerPoint file more colorful and attractive. In this paper, we propose a steganographic method to embed message in a PowerPoint file via various effects. In contrast to other steganographic methods, we not only hide message naturally but also keep the content of the cover media intact. Furthermore, the proposed method can resist the format conversion attack. The experiment result demonstrates that the proposed method is undetectable under some visual and statistical attacks.

Keywords Steganography · PowerPoint file · Animation effects · Timing effects · Transition effects

1 Introduction

With digital data widely used, data hiding techniques have been studied in communicative security. Based on various applications, data hiding techniques can be divided into two categories, one is watermarking, usually applied in copyright protection, and the other is steganography [7], used in privacy communication. Many steganographic methods [3, 5, 8–10, 12, 17] use various digital materials to cover privacy massage. Zou and Shi [17] used inter-word space to conceal massage in an electronic document. Chou and Ramchandrad [3] proposed an audio hiding method that embeds data imperceptibly in a digital audio recording. The popular cover media in steganography is images. Liu et al. [12] and Lee and Chen [10] proposed the typical data hiding approach that insert secret message in the least significant bits (LSBs) of pixels in a digital image. However, the LSB insertion method is vulnerable to lossy compression. Hu proposed a method [5] to embed secret message based

W.-C. Yang · L.-H. Chen (✉)
Department of Computer Science, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu, Taiwan 300, Republic of China
e-mail: lhchen@cc.nctu.edu.tw

W.-C. Yang
e-mail: wchy@debut.cis.nctu.edu.tw

Published online: 01 October 2013

on vector quantization. Lee and Chen proposed a method [8] to embed secret message in objects of images. They presented another steganography approach [9] for JPEG images, the embedded message can survive after the stego image is compressed. Note that all JPEG based methods are vulnerable to lossy recompression and format conversion [4]. Moreover, most of steganographic methods acquire good performance of secret communication but cause little distortion of cover materials.

Recently, some reversible (lossless) steganographic methods [2, 11, 13–16] were proposed. Ni et al. [13] proposed a reversible method that slightly modifies pixel gray levels based on image histogram to hide secret data. Chang et al. [2] proposed a reversible steganographic scheme based on side match vector quantization for compressed images. Lee et al. [11] proposed a reversible steganographic method based on expanding difference between the median and other points in a pixel block. Zhang [16] proposed a reversible data hiding method to hide secret message in an encrypted image. Qin et al. proposed two reversible data hiding methods, one is based on prediction-error expansion [14] and the other is based on image inpainting [15]. Although, these methods can reconstruct the cover media, they distort the stego media. Furthermore, all reversible methods are vulnerable to lossy compression and format conversion.

Microsoft PowerPoint is a ubiquitous presentation program created by Microsoft Company and widely used by businesspeople, researchers, and educators. The program provides users two kinds of effects, animation effects and slide transition effects, to create animations, which are used to liven up on-screen presentations. Jing, Yang and Chen [6] used different animation timing effects to represent different messages. Since most animations are not used, the capacity is low. In this paper, a method is proposed to embed secret message in a PowerPoint file via various animations. Since any animation does not alter the content of a PowerPoint file, the real content of the file can be kept intact. Moreover, the proposed method can resist the format conversion attack and is undetectable.

In the remaining of the paper, the animations of Microsoft PowerPoint 2007 software are described in Section 2. The proposed method is described in Section 3. The analysis of user habits of using animations, the embedding capacity and the security issue are given in Section 4. Conclusion is made in the last section.

2 Animations of Microsoft PowerPoint

As mentioned previously, Microsoft PowerPoint program provides animation and slide transition effects. There are 199 different animation effects, which can be grouped into four categories: Entrance, Emphasis, Motion Paths and Exit. Entrance effects can be applied to objects so that objects enter with animations during Slide-Show. Emphasis effects animate objects on the spot. Motion Paths effects allow objects to move around the Slide-Show. Exit effects allow objects to leave the Slide-Show with animations. Since effects of Emphasis and Motion Paths categories are presented after Entrance effects and before Exit effects, we regroup animation effects into three categories: Entrance, Emphasis/Motion Paths, and Exit. One effect selected from each category is shown in Figs. 1, 2 and 3.

Each animation effect includes several operations. Table 1 lists these operations.

Slide transition effects are used when advancing from one slide to another. There are 58 different slide transition effects. Each slide transition effect contains four operations, which are speed, sound, switch and time. The speed operation controls the showing speed of a slide transition effect in Slide-Show. The sound operation decides the sound when a slide transition effect is presenting. The switch operation decides the way to trigger a slide

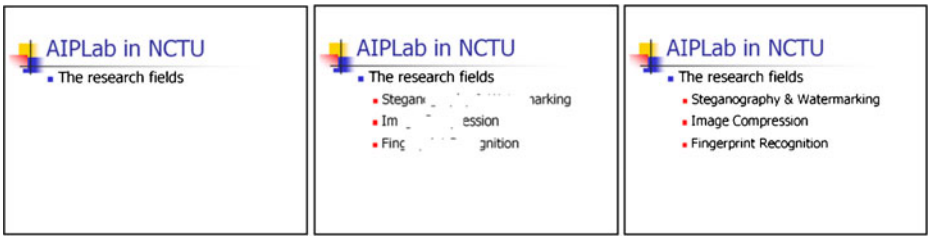


Fig. 1 The "Box" effect of "Entrance" category

transition effect in Slide-Show. The time operation controls the starting time of a slide transition effect after the trigger in Slide-Show.

Figure 4 shows an example of slide transition effects. Figure 4a shows the current slide and Fig. 4d shows the next slide. Figure 4b and c show the intermediate results of applying the "Uncover Down" slide transition effect to Fig. 4d. Note that this effect keeps slide content intact.

3 The proposed method

The proposed method uses animations to represent different messages. To reach this aim, a codebook is first designed to record the correspondence between animations and pieces of message. In addition, automatically applying animations in a PowerPoint file is impossible and not practical. An interactive system is then designed to semi-automatically transform the secret message to animations based on the designed codebook. The proposed method contains two parts: embedding process and extracting process.

3.1 Codebook design

In the codebook design, three types of effects are used to embed message. The first type called animation-based effects is composed of animation effects, each of which contains an animate operation, a direction operation, and a speed operation. The second type called timing-based effects is composed of delay operations, each of which is a delay operation on an animation effect. The third type called transition-based effects is composed of slide transition effects, each of which contains a speed operation and a time operation. The starting time of a slide transition effect controlled by a time operation can be set from

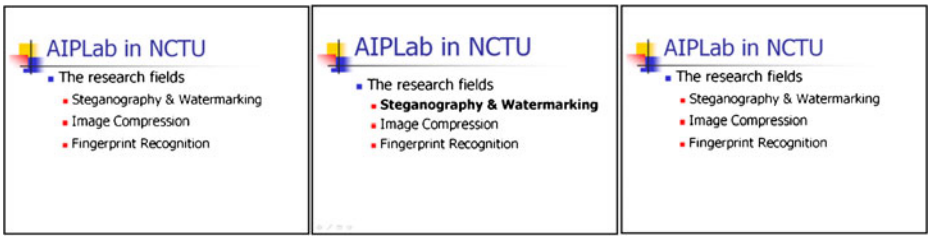


Fig. 2 The "Bold Flash" effect of "Emphasis/Motion Path" category

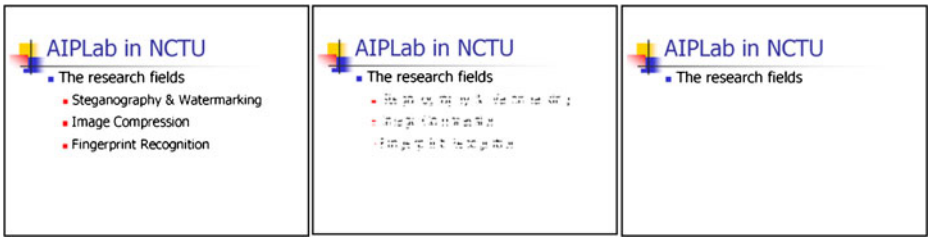


Fig. 3 The "Checkerboard" effect of "Exit" category

00:00:00.00 to 23:59:59.99, that is, from 0 s to 24 h. Note that only the two least significant bits (LSBs) of seconds in the starting time of a time operation are used to embed message.

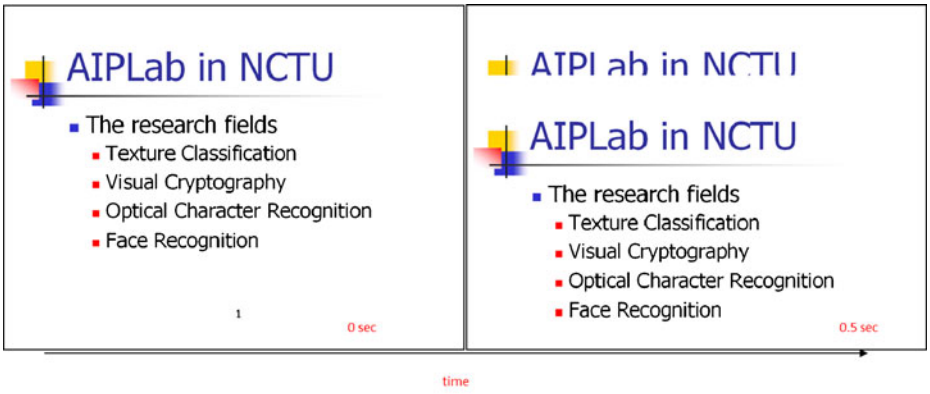
Each type of effects has a corresponding codebook. In each codebook design, each effect stands for a piece of *n*-bit message. In order to make Slide-Show look natural, in the animation-based codebook, each *n*-bit message should have a corresponding effect in each category of animation effects. The reason is that if an *n*-bit message only corresponds to an animation effect, for example, an "Exit" animation, and when we want to embed the message and the current slide is just appearing, we now enforce to add an "Exit" animation, this will make the slide presentation unusual. Here, we give an example of codebook design shown in Tables 2, 3 and 4. Each of animation-based and transition-based effects represents a 3-bit message, and each of timing-based effects represents a 2-bit message.

3.2 The interactive system

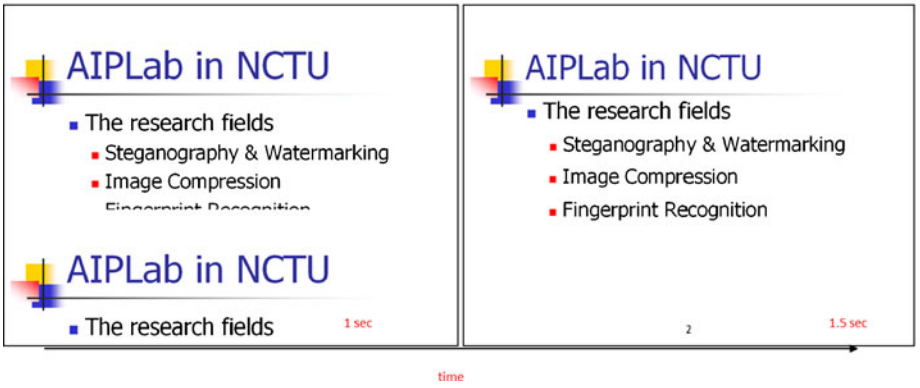
Note that to embed message automatically through effects is impossible, since the added effects should look natural. Here, we use Delphi 7 and Microsoft Access software to develop an interactive system as an assistant for embedding and extracting. Without loss of generality, based on Tables 2, 3 and 4, we give an example to do explanation. In this scenario, three codebooks are designed for three different animations categories. The sender and receiver share the same codebooks before communication. The assistant interfaces of embedding and extracting processes are shown in Figs. 5 and 6, respectively.

Table 1 The list of animation effect operations

Operations
Animate
Direction (if has)
Sound
After animation
Animate text (for text object)
Start
Delay
Speed
Repeat
Group text



(a) The current slide. (b) The intermediate result after 0.5 sec.



(c) The intermediate result after 1 sec. (d) The next slide.

Fig. 4 The "Uncover Down" slide transition effect used. **a** The current slide. **b** The intermediate result after 0.5 s. **c** The intermediate result after 1 s. **d** The next slide

The embedding interactive system contains two phases. In the first phase, a sender inputs the secret message M and the secret key k. Then based on the secret key k, the interactive system converts M into M' using the following equation:

$$M'(i) = M(i) \oplus RS(k, i), \tag{1}$$

where $M'(i)$ and $M(i)$ denote the ith bit of M' and M, respectively. $RS(k,i)$ denotes the ith bit of a pseudo-random generated binary sequence RS using the secret key k as seed. $\oplus$ denotes the exclusive or operation.

In the second phase, the sender first chooses a codebook in the embedding assistant interface (see Fig. 5). Next, the interactive system takes 3 or 2 bits of M' from left to right sequentially based on the chosen codebook. The embedding assistant interface then suggests the corresponding animations. Based on the status of the current slide, the sender can choose a proper effect to do data embedding. The second phase is repeated until all bits of M' are embedded.

In the extracting assistant interface (see Fig. 6), the receiver first inputs the extracted effect, the interactive system will convert the effect into the corresponding 3 or 2 bits of M'.

Table 2 An animation-based codebook using 3 bits to represent an effect with "X" standing for "unnecessary items"

Animation-based effects									
Message (bits)	Entrance			Emphasis/motion path			Exit		
	Animate	Direction	Speed	Animate	Direction	Speed	Animate	Direction	Speed
001	Fly in	Top/ bottom	Slow	Spin	360° clockwise	Slow	Fly out	Top/ bottom	Slow
010	Fly in	Top/ bottom	Medium	Spin	360° clockwise	Medium	Fly out	Top/ bottom	Medium
100	Fly in	Top/ bottom	Fast	Spin	360° clockwise	Fast	Fly out	Top/ bottom	Fast
101	Fly in	Top/ bottom	Very fast	Spin	360° clockwise	Very fast	Fly out	Top/ bottom	Very fast
110	Fly in	Left/right	Slow	Flash bulb	X	Slow	Fly out	Left/right	Slow
011	Fly in	Left/right	Medium	Flash bulb	X	Medium	Fly out	Left/right	Medium
000	Fly in	Left/right	Fast	Flash bulb	X	Fast	Fly out	Left/right	Fast
111	Fly in	Left/right	Very fast	Flash bulb	X	Very fast	Fly out	Left/right	Very fast

After all effects are input, all extracted bits are concatenated into *M'*. Finally, the receiver inputs the secret key *k* to convert *M'* into the secret message *M*.

3.3 Embedding process

Before describing the embedding process, we discuss some observed phenomena when a user adds animations in a PowerPoint file. Then, according to these phenomena, we will give four embedding rules which should be followed by the proposed embedding process. The first phenomenon is that effects of "Emphasis/Motion Paths" and "Exit" animation categories can only be added to an existing object on a slide. The second phenomenon is that if an

Table 3 A transition-based codebook using 3 bits to represent an effect

Transition-based effects			
Message (bits)	Slide transition effect	Speed	The two LSBs of seconds in a time operation
001	Random transition	Medium	00
010	Random transition	Medium	01
100	Random transition	Medium	10
101	Random transition	Medium	11
110	Random transition	Fast	00
011	Random transition	Fast	01
000	Random transition	Fast	10
111	Random transition	Fast	11

Table 4 A timing-based codebook using 2 bits to represent a delay operation of an animation effect

Timing-based effects	
Message	Delay operation (secend)
00	0.5
01	1
10	2
11	2.5

object appears with an effect of "Entrance" animation category, then no more entrance effect can be added to the object. The third phenomenon is that if an object is emphasized with an effect of "Emphasis/Motion Paths" animation category, only exit effects can be added to the object. The fourth phenomenon is that objects with the same level usually contain the same animation effect. A slide with two level objects is shown in Fig. 7. Most academic PowerPoint files belong to this category.

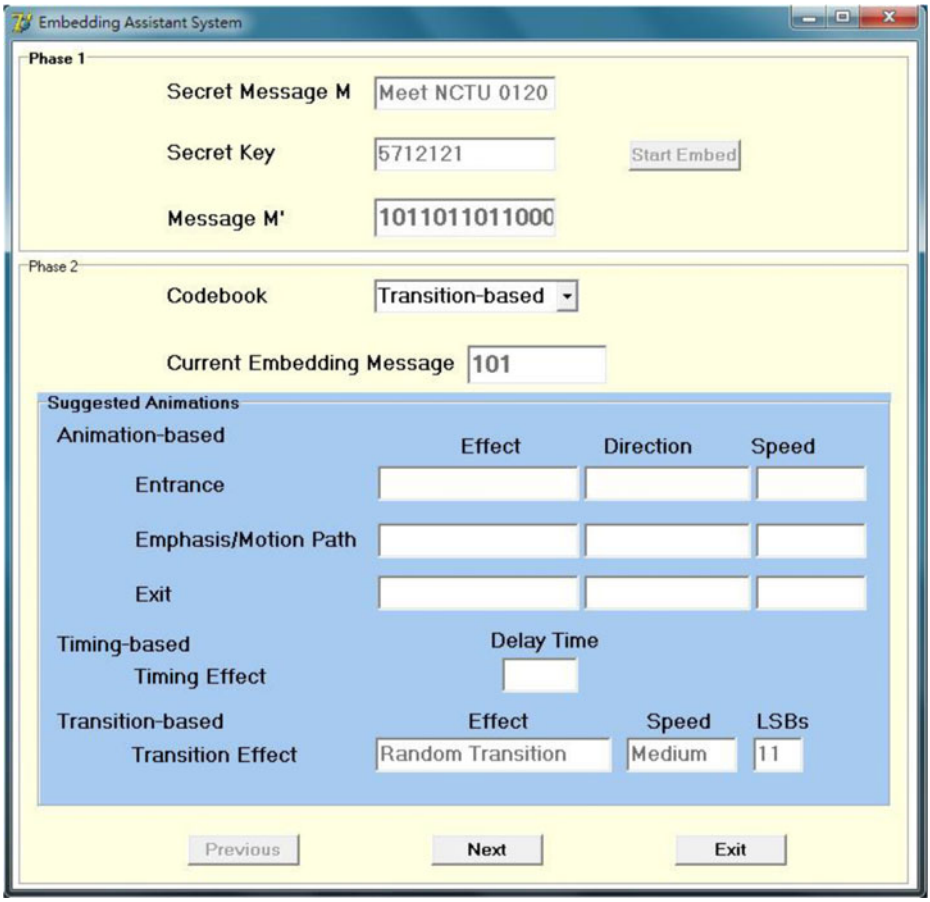


Fig. 5 The embedding assistant interface

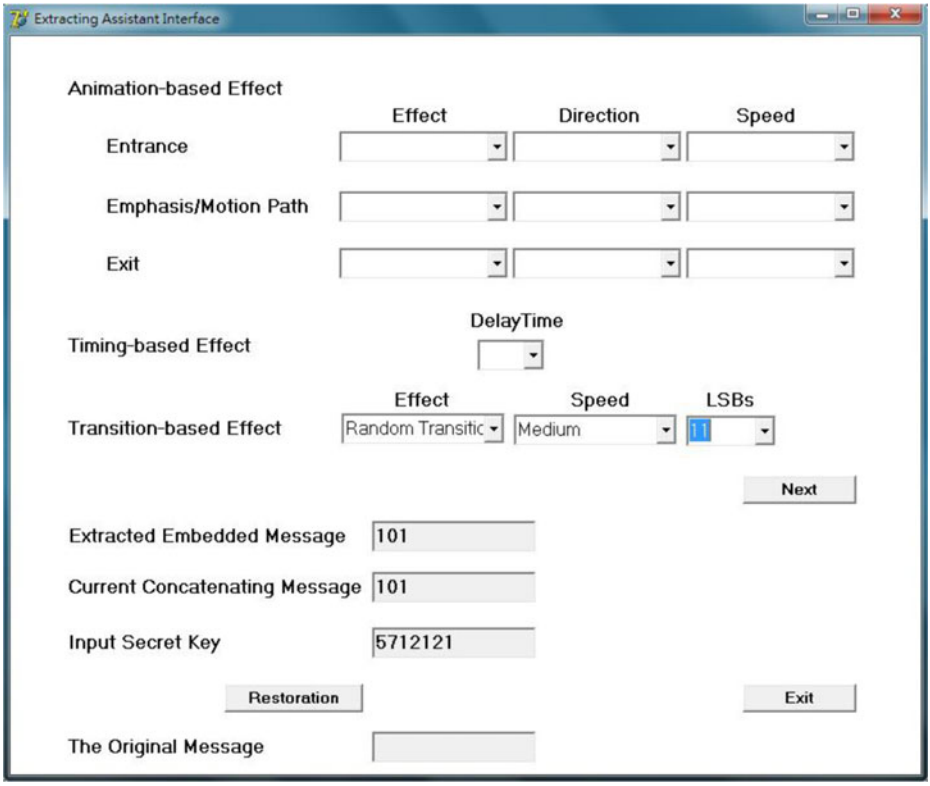


Fig. 6 The extracting assistant interface

According to the observed phenomena, four embedding rules should be obeyed in the embedding process and are given as follows:

Rule 1: If an object used for embedding message is not on a slide, only effects of the "Entrance" animation category can be added.

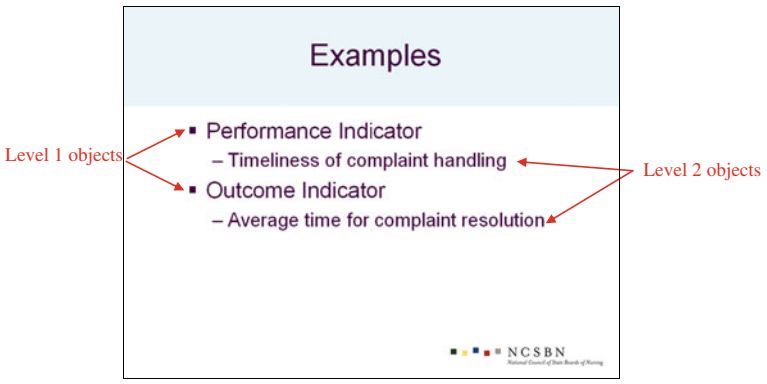


Fig. 7 A slide with two level objects

Rule 2: If an object used for embedding message has embedded a message through an effect of "Entrance" animation category, only effects of "Emphasis/Motion Paths" or "Exit" animation category can be chosen to embed message.

Rule 3: If an object used for embedding message has embedded a message through an effect of "Emphasis/Motion Paths" animation category, only effects of "Exit" animation category can be used to embed message.

Rule 4: The animation effect which contains direction and speed operations should be the same when applying to the same level objects in a slide.

In the embedding process, we need four materials to create the stego PowerPoint file. The first is the secret message M. The second is the secret key k which is used to generate a pseudo-random binary sequence to convert the secret message M into a random binary sequence M'. The main purpose of using the secret key k is to make the appearing probabilities of pieces of message uniform. The third is the chosen codebooks which record the correspondences among pieces of message and effects. The last is the cover media, a PowerPoint file, which will be used to embed secret message. In the following, we will describe the embedding steps in detail.

Embedding procedure

Step 1 Input the secret message M.

Step 2 Use the secret key k as a seed to generate a pseudo-random binary sequence RS. Then use Eq. (1) to convert M into M'.

Step 3 Take an adaptive PowerPoint file.

Step 4 According to the status of the current slide, choose a proper codebook.

Step 5 Based on the codebook, take a piece of M' sequentially, all corresponding effects will be suggested.

Step 6 Based on the status of the current slide, one of the suggested effects is chosen and applied on a proper object or slide.

Step 7 Repeat Steps 4–6 until all bits of M' are embedded.

Note that each object can be applied at most three animation effects, one belongs to the "Entrance" animation category, one belongs to "Emphasis/Motion Paths" animation category, and the other belongs to "Exit" animation category.

3.4 Extracting process

In the extracting process, we need three materials to extract the secret message. One is the same codebooks used in the embedding process. The second is the shared secret key k. The last is the stego PowerPoint file. The steps of the extracting process are described as follows:

Extracting procedure

Step 1 Take the shared codebooks used in the embedding process.

Table 5 The percentages of four categories with "X" standing for "unnecessary items"

Categories	Files with no effect	Files with slide transition effects	Files with simple animations	Files with complex animations
Percentages (%)	56.00	17.67	22.67	3.67
Average number of slides in one file	X	30	35	41
Average number of objects in one file	X	X	90	195

Table 6 Six animation effects with the highest probabilities in each animation category

Entrance effects			Emphasis/motion path effects			Exit effects		
Effects	Probability	Normalized probability	Effects	Probability	Normalized probability	Effects	Probability	Normalized probability
Fly in	21.60 %	47.41 %	Spin	46.94 %	58.97 %	Fly out	12.70 %	27.34 %
Wipe	7.17 %	15.74 %	Grow/ shrink	16.33 %	20.52 %	Pinwheel	7.94 %	17.09 %
Fade	6.91 %	15.17 %	Change fill color	6.12 %	7.69 %	Dissolve out	7.94 %	17.09 %
Blinds	4.15 %	9.11 %	Wave	4.08 %	5.12 %	Wedge	7.94 %	17.09 %
dissolve in	3.44 %	7.55 %	Diamond	4.08 %	5.12 %	Blinds	4.97 %	10.70 %
Rise up	2.29 %	5.02 %	Change line color	2.05 %	2.58 %	Ease out	4.97 %	10.69 %
Total	45.56 %	100 %	Total	79.60 %	100 %	Total	70.27 %	100 %

Table 7 Six slide transition effects with the highest probabilities

Slide transition effects	Probability	Normalized probability
Random transition	14.69 %	30.41 %
Fade smoothly	11.10 %	22.98 %
Cover right	7.19 %	14.89 %
Dissolve	5.52 %	11.43 %
Wipe right	5.15 %	10.66 %
Stripis right-down	4.65 %	9.63 %
Total	48.30 %	100 %

Step 2 Extract effects according to the appearing sequence in Slide-Show from the stego PowerPoint file.
Step 3 Use the interactive system to get the corresponding message piece of each extracted effect.
Step 4 Concatenating all extracted pieces into *M'*.
Step 5 Use the shared secret key *k* to convert *M'* to the secret message *M*.

4 Analysis of the proposed method

In this section, the usage habits of animations by general users are first analyzed. Then the embedding capacity is addressed. Finally, the limited robustness and undetectability are discussed.

4.1 Analysis of animations used by general users

In order to understand user habits of using animations, we analyze 300 PowerPoint files downloaded from the Internet. These files include academic, commercial, political and other topics. They are grouped into four categories; the first has no effect, the second has only slide transition effects, the third contains simple animations, all objects in a PowerPoint file have the same animation-based effect with various timing-based effects, and various slide transition effects are used, and the fourth contains complex animations with various animation-based

Table 8 The probabilities of different delay operations of animation effects

Delay (second)	Probability	Delay (second)	Probability
1	50.71 %	7	0.95 %
2.5	20.38 %	8	0.95 %
2	6.16 %	0.6	0.47 %
0.5	5.69 %	4	0.47 %
1.5	4.27 %	6	0.47 %
3	3.32 %	11	0.47 %
3.5	1.90 %	12	0.47 %
5	1.90 %	30	0.47 %
0.2	0.95 %		

Table 9 The probabilities of entropy values in entrance animation effects

Entropy value range	Files with entrance animation effects
0~0.5	0
0.5~1	0
1~1.5	18.18 %
1.5~2	27.27 %
2~2.5	0
2.5~3	27.27 %
3~3.5	18.18 %
3.5~4	9.10 %

effects, timing-based effects, and slide transition effects. Table 5 shows the percentages of the four categories.

By observing appearing probabilities of animation and slide transition effects in the downloaded 300 PowerPoint files, we find that there are at most six different animation effects and six different slide transition effects in most of the downloaded files. Some files use more than five different animation effects and five different slide transition effects. Tables 6 and 7 list six animation effects and six slide transition effects with the highest probabilities, respectively. The probabilities of delay operations of animation effects are shown in Table 8.

Here, we use entropy to analyze user habits of applying animation, slide transition and delay effects in PowerPoint files. For each PowerPoint file f, we calculate the entropy value, E_f, of effects used as follows:

$$E_f = -\sum P_i log_2 P_i,$$

where P_i stands for the probability of the ith effect used in f. Different entropies stand for different distribution.

Tables 9, 10, 11, 12 and 13 list the probabilities of entropy values for different effect categories. From these Tables, we find that users do not use similar probability models of effects. This means that user habits of applying effects are subjective.

4.2 Embedding capacity

The embedding capacity of the proposed method depends on the number of animations used in a PowerPoint file. As shown in Table 5, PowerPoint files can be divided into four categories according to the usage of animations. Based on Table 5, if the codebooks in

Table 10 The probabilities of entropy values in emphasis/motion path animation effects

Entropy value range	Files with emphasis/motion path animation effects
0~0.5	0
0.5~1	25 %
1~1.5	25 %
1.5~2	25 %
2~2.5	0
2.5~3	25 %

Table 11 The probabilities of entropy values in exit animation effects

Entropy value range	Files with exit animation effects
0~0.5	0
0.5~1	0
1~1.5	0
1.5~2	50 %
2~2.5	0
2.5~3	50 %

Tables 2, 3 and 4 are used, the second category (files with slide transition effects) can embed 3 bits via a transition-based effect, the average capacity for a file in this category is about 90 (30×3) bits, and this is enough for transferring a date or an attacking target information. The third category (files with simple animations) can embed 3 bits via one transition-based effect on a slide and 2 bits via one timing-based effect on an object, the average capacity is about 285 (35×3+90×2) bits, and this is enough for transferring a command. Because all animation-based effects on objects in the third category PowerPoint file are the same, we cannot embed message via animation-based effects. The last category (files with complex animations) can embed 3 bits via one transition-based effect on a slide, 3 bits via one animation-based effect and 2 bits via one timing-based effect on an object. Note that each object can have three animation effects from three animation categories, and each effect can have a timing-based effect. The average capacity is about 3048 (41×3+195×3×3+195×3×2) bits, and this is enough for transferring a secret key. The capacities with different numbers of message bits embedded by an effect are shown in Table 14. In Table 14, each effect represents a k-bit message. Thus, if k=3, based on the average number of slides and objects in Table 5, the average capacity for a file in the second category (file with slide transition effects) is about 90 (30×3) bits, in the third category (files with simple animations) is about 375 (35×3+90×3) bits, and in the fourth category (files with complex animations) is about 3633 (41×3+195×3×3+195×3×3) bits. Users can design codebooks based on the lengths of the secret messages. An example of a stego PowerPoint file is given in [1].

4.3 Limited robustness

As mentioned previously, most of steganographic methods cannot resist to format conversion [4]. The PowerPoint Slide-Show format (.pps) and the Mine-html format (.mht, the web

Table 12 The probabilities of entropy values in slide transition effects

Entropy value range	Files with slide transition effects	Files with simple animation	Files with complex animation
0~0.5	19.05 %	37.50 %	33.33 %
0.5~1	47.60 %	43.75 %	33.33 %
1~1.5	4.77 %	6.25 %	0
1.5~2	4.77 %	6.25 %	33.33 %
2~2.5	14.28 %	0	0
2.5~3	4.77 %	6.25 %	0
3~3.5	4.77 %	0	0

Table 13 The probabilities of entropy values in delay operations of animation effects

Entropy value range	Files with simple animation	Files with complex animation
0~0.5	30.77 %	0 %
0.5~1	38.46 %	50 %
1~1.5	23.07 %	40 %
1.5~2	7.70 %	10 %

archive format) are usually used to broadcast or communicate a PowerPoint file on the Internet. Even in the .pps or .mht file format, the Slide-Show is still the same. This means that the proposed method is robust to format conversion (ppt to pps or ppt to mht).

4.4 Security/undetectability

Security refers to the inability of an eavesdropper to detect hidden information. In practice, a steganographic scheme is considered secure if no existing attack can be modified to build a detector that would be able to distinguish between cover and stego media with a success better than random guessing [4].

In this subsection, we will show that the proposed method is immune from some visual and statistical attacks. Note that in animation-based codebook design, each n-bit message has a corresponding effect in each category of animation effects. Thus, in the embedding process, the sender can adaptively choose a proper effect for each n-bit message via the proposed interactive system. This makes animations on a stego PowerPoint file look natural. That is, the proposed method is visually undetectable.

As to statistical undetectability, Cachin [4] proposed a definition for a secure stegosystem. If the distribution of stego works is identical to the cover works' distribution, the stegosystem is perfectly secure. However, to collect all cover works is impossible. The cover works' distribution cannot be obtained in practice. Here, we compare the probability distribution of animations used in a stego PowerPoint file with that used in a general PowerPoint file. To reach this aim, the entropy value of a probability distribution is used. We do some experiments in each category except the first category (files with no effects) of PowerPoint files. 100 stego PowerPoint files are created based on the previous defined codebooks. The ranges of entropy values of 5 effect types of these stego PowerPoint files are shown in Table 15. All entropy values of the experimental results meet the previous analysis results of user habits shown in Tables 9, 10, 11, 12 and 13.

Table 14 The capacities with different numbers of message bits embedded by an effect

The number of message bits embedded by an effect	Categories of PowerPoint files		
	File with only slide transition effects	Files with simple animations	Files with complex animations
	Capacity (bits)		
3	90	375	3633
4	120	500	4844
5	150	625	6055
6	180	750	7266

Table 15 The entropy values of five types of 100 stego PowerPoint files using the proposed method with "X" standing for "unnecessary items"

Category	Files with only slide transition effects	Files with simple animations	Files with complex animations
	Entropy values		
Slide transition effects	0.7219~1.0000	0.9224~1.0000	0.9848~1.0000
Entrance animation effects	X	X	1.9803~1.9999
Emphasis/motion path animation effects	X	X	0.9878~1.0000
Exit animation effects	X	X	1.9787~1.9999
Delay effects	X	1.0323~1.5656	1.2119~1.5296

For example, files in slide transition effect category have entropy values between 0.7219 and 1.0000 for distributions of slide transition effects, and these values lie in the entropy value range (0.5~1) which is the most frequent usage of users as shown in Table 12. The ranges of entropy values for distributions of delay time effects are (1.0323~1.5656) for simple animations and (1.2119~1.5296) for complex animations, these values lie in the range (1~2), which occupies 50 % probability of users usage as shown in Table 13. Experimental results show that the proposed method is statistically undetectable under entropy comparison.

5 Conclusion

In this paper, we proposed a steganographic method via animation and transition effects in PowerPoint files. In contrast to other steganographic methods, our method does not distort the content of a PowerPoint file and can naturally hide information in files. Furthermore, the proposed method can resist the format conversion attack. Experiment result demonstrates that the proposed method is undetectable under some visual and statistical attacks.

Acknowledgment This work is supported in part by National Science Council of Republic of China under grant NSC-100-2221-E-009-140-MY2.

References

1. A stego PowerPoint file example. http://debut.cis.nctu.edu.tw/stego.pps
2. Chang CC, Tai WL, Lin CC (2006) A reversible data hiding scheme based on side match vector quantization. IEEE Transaction on Circuits System Video Technology 16(10):1301–1308
3. Chou J, Ramchandrad K (May 2001) "Next generation techniques for robust and imperceptible audio data hiding." In: Proc. of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing, vol. 3, pp 1349–1352, Salt Lake City, UT, USA
4. Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T (2008) Digital watermarking and steganography. Morgan Kaufmann Publisher, pp 429–495
5. Hu YC (2006) High-capacity image hiding scheme based on vector quantization. Pattern Recogn 39(9):1715–1724
6. Jing MQ, Yang WC, Chen LH (July 2009) "A new steganography method via various animation timing effects in PowerPoint files." Int Conf Mach Learn Cybern 12–15
7. Katzenbeisser S, Petitcolas FAP (2000) Information hiding techniques for steganography and digital watermark. Artech House, Inc., Massachusetts

8. Lee Y-K, Chen L-H (2002) Object-based image steganography using affine transformation. Int J Pattern Recognit Artif Intell 16(6):681–696
9. Lee Y-K, Chen L-H (2003) Secure error-free steganography for JPEG images. Int J Pattern Recognit Artif Intell 17(6):967–981
10. Lee Y-K, Chen L-H (June 2000) "High capacity image steganographic model." In: IEE Proc. on Vision, Image, and Signal Processing, vol. 147, issue. 3, pp 288–294
11. Lee C-C, Wu H-C, Tsai C-S, Chu Y-P (2008) Adaptive lossless steganographic scheme with centralized difference expansion. Pattern Recogn 41(6):2097–2106
12. Liu S-H, Chen T-H, Yao H-X, Gao W (August 2004) "A variable depth LSB data hiding technique in images." In: Proc. of Int. Conf. on Machine Learning and Cybernetics, vol.7, pp 3990–3994, Shanghai, China
13. Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. IEEE Trans Circ Syst Video Technol 16(3):354–362
14. Qin C, Chang CC, Liao LT (2012) An adaptive prediction-error expansion oriented reversible information hiding scheme. Pattern Recognit Lett 33(16):2166–2172
15. Qin C, Wang ZH, Chang CC, Chen KN (2012) Reversible data hiding scheme based on image inpainting. Fundam Inform 120(1):59–70
16. Zhang XP (2011) Reversible data hiding in encrypted image. IEEE Signal Proc Lett 18(4):255–258
17. Zou D, Shi YQ (May 2005) "Formatted text document data hiding robust to printing, copying and scanning". In: Proc. of IEEE Int. Symposium on Circuits and Systems, vol. 5, pp 4971–4974, Kobe, Japan

Wen-Chao Yang was born in Taoyuan, Taiwan, Republic of China on June 27, 1975. He received the B.S. degree in Department of Criminal Investigation from Central Police University, Taoyuan, Taiwan in 1997 and M.B.A. degree in Department of Information Management from National Central University, Taoyuan, Taiwan in 2002. He is now a Ph.D. Candidate of College of Computer Science at National Chiao Tung University, Hsinchu, Taiwan. His major research interests include image processing, data hiding, forensic.

Ling-Hwei Chen was born in Changhua, Taiwan, in 1954. She received the B.S. degree in Mathematics and the M.S. degree in Applied Mathematics from National Tsing Hua University, Hsinchu, Taiwan in 1975 and 1977, respectively, and the Ph.D. degree in Computer Engineering from National Chiao Tung University, Hsinchu, Taiwan in 1987.

From August 1977 to April 1979 she worked as a research assistant in the Chung-Shan Institute of Science and Technology, Taoyan, Taiwan, From May 1979 to February 1981 she worked as a research associate in the Electronic Research and Service Organization, Industry Technology Research Institute, Hsinchu, Taiwan. From March 1981 to August 1983 she worked as an engineer in the Institute of Information Industry, Taipei, Taiwan. She is now a Professor of the Department of Computer Science at the National Chiao Tung University. Her current research interests include image processing, pattern recognition, Multimedia compression, content-based retrieval and Multimedia Steganography.