An Application of Visual Cryptography To Financial Documents

L. W. Hawkes, A. Yasinsac, C. Cline
Security and Assurance in Information Technology Laboratory
Computer Science Department
Florida State University
Tallahassee, FL 32306-4530

Keywords: visual cryptography, financial security, greying effect, network security

Abstract: VCRYPT, an application of visual cryptography, is described as a means of transmitting financial documents where moderate security is required. Visual cryptography in general uses a simple algorithm unlike the complex, computationally intensive algorithms used in other techniques. The interface to the system is window based. The VCRYPT implementation solves the outstanding problem of the *greying effect* in which the decoding results in a distinctly "grey" or fuzzy version of the source document. Thus, when visual cryptography is applied to financial documents, it is often difficult to distinguish digits accurately, making it an unattractive protection technique. VCRYPT overcomes this problem using a threshold technique to produce a clear, crisp document, identical to the original. Although visual cryptography requires increased storage and multiple transmissions, the simple share creation algorithm, decreasing storage costs, and fast transmission times, make this a viable alternative for sharing financial documents over the Internet.

1. Introduction

With the near universal use of the Internet in business, the need to share financial documents via this medium becomes increasingly more necessary. We introduce VCRYPT [5], a simple, fast, visual cryptography technique, to provide privacy protection when transmitting sensitive data between offices. This technique also makes it difficult for the recipient to modify the source, maintaining the authenticity of the document. Moreover, the final image can be obtained simply with the human visual system. The associated storage cost is increased with this method, but with overall memory and disk storage costs continually decreasing, this issue becomes less significant.

This approach is particularly applicable in situations where a moderate degree of security is required when sharing sensitive financial documents over the Internet. Like other threshold schemes, visual cryptography can be used to protect secrecy or it may be used to ensure that a given subset of compromised principals can neither retrieve the secret, nor can they prevent honest principals from receiving the secret.

VCRYPT takes a financial document (spreadsheet, for example) represented as a bit map file, and expands it into two or more encoded file shares. These shares can be transferred to the recipients via electronic mail or electronic file transfer process, such as ftp. In order to recover the original document, the recipient only need have the desired subset of the shares and the decoding program.

Other visual cryptography techniques have cumbersome user interfaces. Using the VCRYPT simple, window-based interface, the encoding style can be selected with one mouse click. Previous visual cryptography systems also suffer from a *greying effect* or the decoded image being blurry and much darker than the original image. This is one reason for the approach not becoming a competitive technique for moderate security applications. Our system removes this problem and precisely reproduces the original document. Although the storage requirements for the document are increased, the computational impact is reduced.

In this section we have introduced visual cryptography, its advantages and its problems. In section 2 we give details of the visual cryptography approach. In the next section we give details of VCRYPT, present a simple example, and discuss how this can be used for financial documents. We conclude with section 4, in which we highlight our contributions and overview future extensions planned.

2. Visual Cryptography

In 1994, Naor and Shamir [3] presented a new cryptographic paradigm based at the pixel level. They termed this *visual cryptography* and introduced it as a method for encrypting such things as handwritten notes, pictures, graphical images, as well as typed text stored as a graphic image. We posit that this technique has characteristics that make it desirable for use in financial transactions conducted over the Internet.

2.1 The Basic Model

The basic 2 out of 2 visual cryptography model consists of a secret message encoded into two transparencies, one transparency representing the ciphertext and the other acting as a secret key. Both transparencies appear to be random dots when inspected individually and provide no information about the original cleartext. However, by carefully aligning the transparencies, the original secret message is reproduced. The actual decoding is accomplished by the human visual system.

Naor and Shamir further describe the visual cryptography scheme as a visual secret sharing problem in which the secret message can be viewed as nothing more than a collection of black and white pixels. Each pixel in the original image is represented by at least one subpixel in each of the $\boldsymbol{n}$ transparencies or shares generated. Each share is comprised of collections of $\boldsymbol{m}$ black and white subpixels where each collection represents a particular original pixel.

An example of the encoding of white and black pixels in a 2 out of 2 scheme can be seen in Figure 1. Here two shares out of the two generated would be needed to recover the original image. Since only two shares are generated, $\boldsymbol{n} = 2$. Figure 1(a) represents a single white or black pixel in the original image. Figure 1(b) represents the subpixel assignments that would be given to shares #1 and #2 respectively. The number of subpixels per share used to represent the original pixel is four ($\boldsymbol{m} = 4$). Finally, Figure 1(c) represents the overall visual effect when shares #1 and #2 are correctly aligned on top of one another. Notice that when the shares in this example are combined the original black pixel is viewed as black, however, the original white pixel takes on a grey scale.

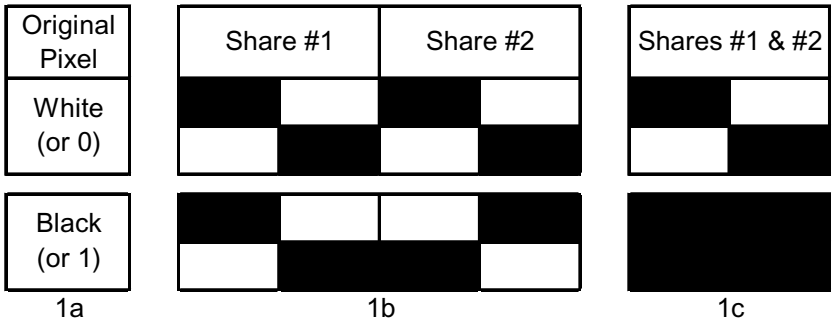

Figure 1

The structure obtained from either white or black pixel representation in Figure 1 can be described by an $\boldsymbol{n}$ x $\boldsymbol{m}$ Boolean matrix $\boldsymbol{S_p}$ where $\boldsymbol{p}$ ε {white, black}. Any given element of the matrix $\boldsymbol{S}$ say s_{ij}, is considered to be 1 iff the *j*th subpixel in the *i*th transparency is black. When the $\boldsymbol{n}$ transparencies are properly aligned,

the resulting black subpixels are the Boolean OR of the columns for each row $i_1, i_2, \ldots, i_n$ of S. Shares #1 and #2 of Figure 1 would represent i_1 and i_2 respectively. Therefore, the following 2 x 4 Boolean matrices would be derived:

$S_{white} = \{ \{1, 0, 0, 1\}, \{1, 0, 0, 1\}\}$ and $S_{black} = \{ \{1, 0, 0, 1\}, \{0, 1, 1, 0\} \}$.

The matrix elements represent share assignments for share #1 and share #2 respectively.

Since m subpixels constitute one original pixel and the overall visual effect of a black subpixel in any one of the shares causes that particular subpixel when combined to become black, inspection of the grey level is the method of determining the original color of a pixel. The grey level of the combined share's subpixels is proportional to the Hamming weight $H(V)$ of the ORed m-vector V. The combined subpixels are interpreted by the human visual system as a black pixel if $H(V) \geq d$ and as a white pixel if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha \Rightarrow 0$. The use of threshold d and relative difference α is necessary in order to distinguish between the colors.

2.2 Solving the *k* out of *n* Visual Secret Sharing Problem.

Naor and Shamir continued by expanding the basic visual cryptography scheme to solve the k out of n visual secret sharing problem. A case where visual cryptography is applied to the k out of n problem could begin with a person generating n shares from an original secret image. These n shares could be distributed via some method, say email, to n different participants with no prior knowledge of their particular share. In order to retrieve the original image, k out of the n participants would have to collaborate and overlay their shares. Any k out of n participants collaborating could reveal the original secret message, but fewer than k participants could reveal no information at all.

This threshold model is similar to that above but also includes two collections of n x m Boolean matrices S_0 and S_1. S_0 acts as a pool of matrices from which to randomly choose matrix S to represent a white pixel while S_1 acts as a pool of matrices from which to randomly choose matrix S to represent a black pixel. The matrix chosen thereby establishes the color of the m subpixels in each one of the n transparencies.

In order to be sure that an infinitely powerful cryptanalyst cannot gain any information on the original image by examining fewer than k transparencies, the following conditions must be in place [4]:

1. For any S in S_0, the OR V of any k of the n rows satisfies $H(V) < d - \alpha m$.
2. For any S in S_1, the OR V of any k of the n rows satisfies $H(V) \geq d$.
3. For any subset $\{ i_1, i_2, \ldots, i_q \}$ of $\{1, 2, \ldots, n\}$ with $q < k$, the two collections of q x m matrices D_t where $t \in \{0, 1\}$ obtained by restricting each n x m matrix in S_t to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that there is no way to determine which D_t is used to generate white pixels and which is used to generate black pixels.

The first two conditions are referred to as *contrast* while the third condition is referred to as *security*.

As indicated above, one of the advantages of visual cryptography is that there is no computation used. Furthermore, decryption is accomplished by aligning the shares and viewing the original image. Moreover, since there is no complex cryptographic algorithm, the time needed to encrypt is minimal.

2.3 Other Extensions

Instead of using the standard k out of n sharing scheme above, Ateniese et al [1] precisely qualified subsets of the n shares that will be able to visually recover the secret image. Any non-qualified shares will have no information concerning the secret image.

The mathematical formulation used in [1] for encryption is similar to that of Naor and Shamir, but with more precise definition and nomenclature. They also use two n x m matrix pools from which to distribute shares corresponding to white or black pixels. S_0 and S_1 are called *basis matrices* for a (k, n) threshold visual cryptography scheme with *pixel expansion* m and *contrast* c provided that the following properties are satisfied for every subset X of $\{i_1, i_2, \ldots, i_p\}$:

1) if $X = \{i_1, i_2, \ldots, i_p\}$ with $p \geq k$, then the OR of rows $i_1, i_2, \ldots, i_p$ of S_1 has weight at least t_x

2) if $X = \{i_1, i_2, \ldots, i_p\}$ with $p \geq k$, then the OR of rows $i_1, i_2, \ldots, i_p$ of S_0 has weight at least $t_x - c$

3) if $X = \{i_1, i_2, \ldots, i_p\}$ with $p \leq k-1$, then the two p x m matrices obtained by restricting S_0 and S_1 to rows $i_1, i_2, \ldots, i_p$ are identical up to a column permutation.

The *grey level* of a black and white pixel respectively is t_x/m and $(t_x - c)/m$. The *relative contrast*, c/m, also plays a very important role in determining the visibility of the image. The larger the relative contrast, the easier it is for the human visual system to clearly pick out distinct outlines in the superimposed image.

3. VCRYPT

The VCRYPT program is designed to allow users to easily transmit drawings and documents over the Internet. The encoding process consists of taking the original image and producing n shares which are saved as individual files. The security gained through visual cryptography requires proper distribution of the shares. For example, instead of attaching all of the shares to one email message, it is better to disburse the shares by sending multiple emails to the different recipients. This forces the recipients to work together to recover the drawing. Since a k out of n scheme is used by the VCRYPT program, the interception of any one share would be of no use. In general, a strategy must be developed when using visual cryptography that takes advantage of the distribution of shares and different transmission techniques. When the image is a spreadsheet, since it is being transmitted as a bitmap, the recipient cannot easily change a digit in the copy.

3.1 The Greying Effect

One of the most obvious limitations of using visual cryptography in the past was the problem of the decoded image containing an overall grey effect due to the leftover black subpixels from encoding. This occurred because the decoded image is not an exact preproduction, but an expansion of the original, with extra black pixels. Black pixels in the original document remain black pixels in the decoded version, but white pixels become grey. This resulted in a loss of contrast to the entire image. The extra black subpixels in the image cause the image to become distorted. This is unacceptable since the digits used in the financial documents must be clearly discernable.

In order to overcome this problem, the VCRYPT program employs a post-receipt threshold filtering technique combined, with resizing, to return the decoded image precisely to its original form. As designed by Naor and Shamir, document shares are combined by the recipient using transparencies, so no post-receipt process is required. In order to filter the greying effect, VCRYPT offers post-receipt processing that can filter the grey pixels and reduce the document precisely to its original form. VCRYPT evaluates every set of m subpixels against the threshold; the pixel is black if the number of black subpixels is above the threshold and white if below the threshold.

3.2 The VCRYPT Program

The main goal of VCRYPT is to take a graphically represented image and encode it into multiple shares. The opposite direction (at the recipient) takes the multiple shares created and reconstructs the original graphical image. Therefore the data flow consists of a graphical file being encoded into multiple files (shares) using some file format. Since the concept of visual cryptography deals with the encoding of pixels into subpixels and collections of Boolean matrices, the natural graphical file format to begin working with is the device independent bitmap or BMP file. The VCRYPT program allows for manipulating the BMP file in various ways and uses a modified version of the BMP file format to store the encoded shares created. Great attention was given to the look and feel of the VCRYPT program. Ease of use coupled with a high quality graphical user interface are necessities in today's software market. In order to keep a sense of familiarity, the VCRYPT program makes use of several standard windows, pull-down menus and buttons. It has standard File, Edit, View, Window, and Help pull-down menus with common menu items on each. Beneath the menu bar is a typical toolbar which gives the user quick access to menu features with just one click of a button. The toolbar buttons include, from left to right, New, Open, Save, Print, Cut, Copy, Paste, Overlay, Encode, Decode, About, and Help. The user interface allows for multiple windows for ease of viewing and provides complete access to the Windows clipboard for Cut, Copy, and Paste operations between different windows applications.

Since the graphical user interface is designed to be familiar and user friendly, the entire visual cryptography process requires little additional knowledge on the user's behalf to operate. Unlike past applications of visual cryptography, which used cumbersome interfaces, this style of user interface immediately promotes visual cryptography's use in a wide range of windows applications.

3.3 Encoding and Decoding

The encoding option can either be found on the toolbar as described above or on the Edit menu. Once selected, a dialog box opens. The user is then presented with three different encoding styles to choose from. The Basic encoding style uses a 2 out of 2 encoding scheme. The second option is Moderate which uses a 3 out of 4 encoding scheme. Finally, the Advanced option makes use of a 4 out of 6 encoding scheme. The generated shares are automatically given the same file name as the original image, but the extensions are of the form VC***p*** where ***p*** is the number of the share created. These files are saved in the same directory as the original image file.

The VCRYPT program uses two Boolean matrix pools as described above to encode the original image into ***n*** shares. Each Boolean matrix pool contains encoding matrices for black and white pixels respectively. The following Boolean matrix pools are those used by the VCRYPT program to encode black and white pixels when the Basic encoding style (2 out of 2) is chosen:

B={{0011 1100}, {0101 1010}, {0110 1001}, {1100 0011}, {1010 0101}, {1001 0110}}

W={{001 10011},{0101 0101}, {0110 0110}, {1100 1100},{1010 1010}, {1001 1001}}.

When a particular matrix from either ***B*** or ***W*** is randomly selected during encoding, the first four bits of the selected matrix are assigned to share #1 and the second four bits are assigned to share #2. Since the encoding forces four bits to represent one original image bit in each share, the resulting share file size will be larger than the original image file.

The decoding option can be also either found on the toolbar or the Edit menu. The entire decoding process involves two separate steps: overlay the shares, and filter the resulting image using an established threshold. The overlay process simply performs a bitwise AND on the shares found in the current directory.

After the decoding process overlays the shares, it begins the filtering by looking at the subpixels that represent the original pixel. After inspection of the subpixels, a threshold is then used to determine whether the pixel in the decoded image will be black or white. This ensures that each pixel in the decoded image will match the original encoded pixel. Until the VCRYPT program, this *greying effect* would not allow any image to be decoded into its original form. This is one reason why visual cryptography has not gained more attention as an alternate form of cryptography.

3.4 The "Hello World" Message

We illustrate the use of VCRYPT with the standard *Hello World* message. The original message, a monochrome bitmap file with dimensions 640 x 480 pixels is shown in Figure 2 Although this is a relatively simple message, it contains a characteristic that can cause problems when visually encoded and decoded: the lack of straight lines. This is why it is often used as an example. The image is encoded using a Basic encoding style of 2 out of 2. This causes two shares to be created and stored in the current directory. These are shown in Figures 3 and 4, which are not to scale.

Figure 2

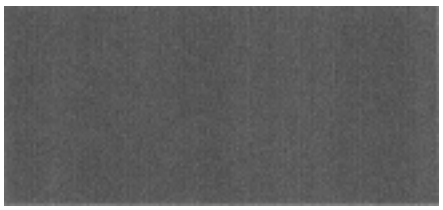

Figure 3. Share #1

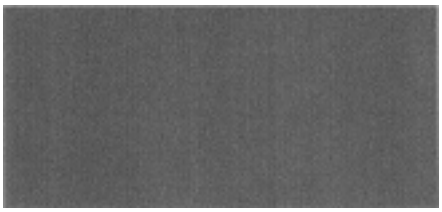

Figure 4. Share #2

Figures 3 and 4 provide no information regarding the original *Hello World* message at all. Each of the shares are monochrome bitmap files with dimensions 1280 x 960 pixels. The increase in dimensions is to allow for the expansion of the image due to encoding.

At this point, we could simply choose to decode the images and get the original *Hello World* image back, but instead we will choose the Overlay option instead. This will cause the VCRYPT program to overlay the two shares, producing Figure 5. This figure demonstrates how the human visual system can decode the shares once they have been overlaid. No decryption algorithm has been used and yet the original message is now visible. However, the *greying effect* is noticeable and would be quite unacceptable with a spreadsheet.

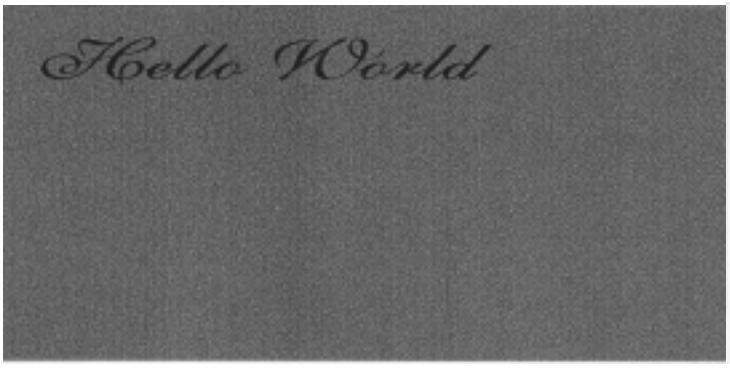

Figure 5

Figure 6

If the Decoding option is selected, the result is given by Figure 6. The final decoded image has all the attributes that the original had, giving a crisp, clear result which would be acceptable when sharing financial documents.

4.0 Contributions.

The VCRYPT visual cryptographic system for transmitting financial documents, with a moderate degree of security, over the Internet has several advantages:

1. complex cryptographic algorithms are not needed;

2. a simple window-based interface is used;

3. the threshold technique, plus resizing, returns the decoded image to its original form i.e. removes the *greying effect*.

The technique also has some disadvantages but these are minor in comparison to the above advantages. The encryption does require increased disk space, but with the falling cost of this resource and the option of compressing files, this aspect of the approach is not significant. Another consideration is that the ***n,*** rather than 1, files (shares) are transmitted. This takes more time but in contrast to the other cryptographic algorithms that are computationally intense, this time is minimal.

Currently, we are enhancing the program in several ways to include:

1. The support of additional file formats,

2. An increase in the number of options for choice of ***k*** and ***n,***

3. An interface with a user's email client of choice,

4. The addition of a watermark on the original document for further security,

5. Varying the encoding matrix choice during encryption to add more security

6. Disguising a share such that it is an "innocent looking picture" while carrying a hidden message.

References:

1. Ateniese, G., C. Blundo, A. De Santis, and D. R. Stinson, Constructions and bounds for visual cryptography, in *23rd International Colloquium on Automata, Languages, and Programming, (ICALP '96)*, Friedhelm Meyer auf der Heide, Ed., Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1996.

2. Mueller, S., *Upgrading and Repairing PCS,* 3rd Edition, Que Corporation, Indianapolis, Indiana, 1993

3. Naor, M. and A. Shamir, Visual Cryptography, in *Advances in Cryptology – Eurocrypt '94*, A. De Santis, Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp 1-12, 1995.

4. Simmons, G. J., *Contemporary Cryptology: The Science of Information Integrity,* IEEE Press, Piscataway, New Jersey, 1992.

5. Cline, Charles A., "A Practical Approach to Using Visual Cryptography in Technical Drawing Environments", Masters Thesis, Florida State University, December 1997