International Journal of Rough Sets and Data Analysis
Volume 6 • Issue 1 • January-March 2019

A New Bi-Level Encoding and Decoding Scheme for Pixel Expansion Based Visual Cryptography

Ram Chandra Barik, National Institute of Technology, Durgapur, India

Suvamoy Changder, National Institute of Technology, Durgapur, India

Sitanshu Sekhar Sahu, Birla Institute of Technology, Mesra, India

ABSTRACT

Mapping of image-based object textures to ASCII characters can be a new modification towards visual cryptography. Naor and Shamir proposed a new dimension of Information security as visual cryptography which is a secret sharing scheme among *N* number of participants with pixel expansion. Later on, many researchers extended the visual secret sharing scheme with no expansion of pixel regions in binary and color images. By stacking *k* shares the secret can be decoded using normal vision. In this paper the authors have proposed a modification towards visual cryptography by converting the message in the form of printable ASCII character-based numerical encoding patterns in a binary host image. The encoding of the message is represented as ASCII numeric and a texture of those numeric are arranged to form a binary host image. Then, *N* numbers of shares are built up but after stacking all the shares the decoding of the message is achieved by converting ASCII numeric to the secret.

KEYWORDS

ASCII Code, Binary Host Image, Lagrange's Interpolation, Visual Cryptography

INTRODUCTION

Demand of information exchange in heavy data traffic is increasing day by day with the influence of digital media over internet. Information security in modern era is a major concern for many mathematicians, computer scientists. For abstracting the secret from malicious access, third party attack there are many algorithms and mathematics was being proposed in last three decade. Usage of Mathematics makes many cryptographic algorithms robust. Today's world is roaming behind the information operated in electronic media and internet technology starting from banking sector (both offline and online banking) to multimedia industry. As advancement of electronic media, digital communication makes the world is in finger press at the same time misuse of information is a big threat to modern world. Cryptography makes the secret information into an unreadable format and plays a vital role in presence of third parties or eavesdropper for secure communication. In the last three decades, popular cryptographic algorithms RSA, AES, DES, Blowfish, Secret Sharing etc. using private key and public key concepts provides security to text-based information. Day by day evolution of digital multimedia information system demands to build new cryptographic algorithm to

DOI: 10.4018/IJRSDA.2019010102

cope with current technological arena. Steganography, Visual Cryptography, QR Code are emerging areas of security over modern multimedia technology. Visual Cryptography combines secret sharing scheme proposed by (Shamir 1979) with visual transparencies into n number of shares. The concept of visual cryptography is combined with visual secret sharing, threshold secret sharing scheme to produce a robust encryption and decryption method which has the broad areas of application. To divide secret data into shares which generate random shares of (k-1) polynomial degree using modulus based arithmetic where ($k \leq n$). f(x) can be derived in equation (1) as

$$f\left(x\right) = \left(a_0 + a_1 x^1 + a_2 x^2 \ldots + a_{k-1} x^{k-1}\right) \bmod p_r \tag{1}$$

Secret data is a_0, p_r is the prime number $p_r > a_0$ and $p_r > n$. From the integer values of uniformly distributed [1; p) the coefficients $\mathrm{a}_1, \mathrm{a}_2 \ldots \mathrm{a}_{k-1}$ are chosen randomly. Mathematically Lagrange's interpolation is used in secret sharing scheme which is represented in equation (2), (3) and (4) using Lagrange's interpolation $\left(x_i, f\left(x_i\right)\right)$, I = 1, 2…n.

$$f\left[x_0, x_1 \ldots, x_n, x\right] = 0 \tag{2}$$

$$\mathrm{f}\left(\mathrm{x}\right) = \frac{\left(\mathrm{x}-\mathrm{x}_1\right)\ldots\left(\mathrm{x}-\mathrm{x}_\mathrm{n}\right)}{\left(\mathrm{x}_0-\mathrm{x}_1\right)\ldots\left(\mathrm{x}_0-\mathrm{x}_\mathrm{n}\right)}\mathrm{f}_0 + \ldots + \frac{\left(\mathrm{x}-\mathrm{x}_0\right)\ldots\left(\mathrm{x}-\mathrm{x}_{\mathrm{n}-1}\right)}{\left(\mathrm{x}_\mathrm{n}-\mathrm{x}_0\right)\ldots\left(\mathrm{x}_\mathrm{n}-\mathrm{x}_{\mathrm{n}-1}\right)}\mathrm{f}_\mathrm{n} = \sum_{\mathrm{i}=0}^{\mathrm{n}}\left(\prod_{\mathrm{j}=0}^{\mathrm{n}}\frac{\mathrm{x}-\mathrm{x}_\mathrm{j}}{\mathrm{x}_\mathrm{i}-\mathrm{x}_\mathrm{j}}\right)\mathrm{f}_\mathrm{i} \tag{3}$$

$$\mathrm{y} = \mathrm{f}\left(\mathrm{x}\right) = \mathrm{secret}\left(\mathrm{s}\right) + \sum_{\mathrm{j}=1}^{\mathrm{k}-1}\mathrm{a}_\mathrm{j}\mathrm{x}^\mathrm{j} \tag{4}$$

Visual Cryptography gives a new dimension to information security arena using secret sharing scheme among a set of trusted participants. Beauty of this security concept is that unlike other highly computational with bigger complexity method such as RSA, AES, DES the decoding of the corresponding secret can be achieve using normal human perception without performing the computation at receivers end. Visual Cryptography has versatile application areas starting from banking sector to other security area.

Secret sharing scheme introduced by Naor and Shamir (Naor & Shamir 1995) is being modified in many dimensions with pixel expansion and no expansion. Binary image with the secret embedding inside black and white pixels intensity or grey level is encoded to form shares using binary patterns randomly. The shares are mapped onto transparencies and distributed between n participants as $\mathrm{P} = \left(\mathrm{P}_1,\ \mathrm{P}_2 \ldots\ \mathrm{P}_\mathrm{n}\right)$. The distribution can be done in such a way to all qualified participants that the original message or secret is visible if k transparencies overlapped or stacked together. The message or secret is invisible when k-1 transparencies stacked even if a highly computational algorithm used. The Qualified participants which holds the share $\Gamma = \left\{\mathrm{Q}_1, \mathrm{Q}_2 \ldots \mathrm{Q}_\mathrm{m}\right\}$ where each Qualified subsets is called as the access structure. (Ateniese, Blundo, DeSantis, Stinson 1999) The extension for Naor and Shamir method towards general Access structures give a new dimension to visual secret sharing scheme. For example, $\mathrm{P} = \left\{\mathrm{S1},\ \mathrm{S2},\ \mathrm{S3}\right\}$ with general access structure are qualified sets at least having two sub-sets as $\left\{\mathrm{S1}, \mathrm{S2}\right\}, \left\{\mathrm{S2}, \mathrm{S3}\right\}$. Whereas overall qualified participants are