Multimedia Tools and Applications (2021) 80:31435–31449
https://doi.org/10.1007/s11042-021-10827-x

1194: SECURED AND EFFICIENT CONVERGENCE OF ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS

Towards an optimized security approach to IoT devices with confidential healthcare data exchange

Andreou Andreas[1] · Constandinos X. Mavromoustakis[1] · George Mastorakis[2] · Dinh-Thuan Do[3] · Jordi Mongay Batalla[4] · Evangelos Pallis[5] · Evangelos K. Markakis[5]

Received: 17 August 2020 / Revised: 26 January 2021 / Accepted: 10 March 2021 /
Published online: 26 March 2021

Abstract
Reliable data exchange and efficient image transfer are currently significant research challenges in health care systems. To incentivize data exchange within the Internet of Things (IoT) framework, we need to ensure data sovereignty by facilitating secure data exchange between trusted parties. The security and reliability of data-sharing infrastructure require a community of trust. Therefore, this paper introduces an encryption frame based on data fragmentation. It also presents a novel, deterministic grey-scale optical encryption scheme based on fundamental mathematics. The objective is to use encryption as the underlying measure to make the data unintelligible while exploiting fragmentation to break down sensitive relationships between attributes. Thus, sensitive data distributed in separate data repositories for decryption and reconstruction using interpolation by knowing polynomial coefficients and personal values from the DBMS Database Management System. Aims also to ensure the secure acquisition of diagnostic images, micrography, and all types of medical imagery based on probabilistic approaches. Visual sharing of confidential medical imageries based on implementing a novel method, where transparencies $\leq k-1$ out of n cannot reveal the original image.

Keywords Visual secret sharing · Confidentiality · Data exchange · Fragmentation · IoT internet of things · Encryption · Cloud computing

1 Introduction

The exchange of health information enables the electronic transfer of clinical data between different health systems and preserving their importance. Facilitate access and retrieval of clinical data to provide safe, timely, effective, and equitable patient-centred care, the World

✉ Andreou Andreas
andreou.andreas@unic.ac.cy

Extended author information available on the last page of the article

Health Organization (WHO) digitally-enabled health systems that place people at the centre of digital health, adopt and use digital health technologies [33]. Therefore, this scope requires countries to empower an integrated patient-centred approach. Innovative technologies integrated via IoT for virtual care and remote monitoring, such as smartphones connected to healthcare platforms, will allow data exchange, storage, and acquisition. The objective is to share information throughout the health ecosystem by creating ongoing care to enhance health outcomes. Of paramount importance to achieve innovation in current digitalization is to unfold the full potential data exchange activity between countries, industries, companies, healthcare systems, etc. To incentivize data exchange, we must ensure data sovereignty by facilitating the secure exchange of data between trusted parties.

The Fast Healthcare Interoperability Resources (FHIR) standard, created by Health Level Seven International (HL7), is currently the most widely used set of protocols for merging different healthcare systems. It is also an Application Programming Interface (API) for interoperability and exchanging health information [20]. Substitutable Medical Apps, Reusable Technologies (SMART) integrated with FHIR to enable healthcare applications connection to Electronic Health Record EHR systems with the appropriate safety guarantees and support authorization, authentication, and User Interface UI integration [26]. FHIR profiles assure SMART applications that resource coding of medication, procedures, conditions, laboratory results, or allergies meet data quality compliance requirements [31]. SMART's integration with FHIR also seeks to restraint significant fragmentation by implementing widely applicable data constraints based on the terms introduced by the US Meaningful Use program [11].

Security and reliability of data-sharing infrastructure require a trusted community; therefore, mutually customized components such as the encryption system are mandatory. Fragmentation is a fundamental cryptographic technique for a data exchange strategy and is also required when COVID-19 deteriorates [6]. This paper proposes distributing fragments to Cloud Repositories (CR) from where the server module will further spread the datasets into separated data repositories. The shares can only be retrieved and reconstruct from the reliable DBMS deployed in the cloud. Thus, this approach improves data privacy and confidentiality during the data exchange process and facilitates the process without further complex encryption techniques. The primary requirement for healthcare innovation is to ensure the confidentiality of the patient's data, stored in the system, or sharing with reliable external parties. The demand for secure image sharing in the healthcare sector has prompted us to include a virtual plan for sharing secret binary images.

The objectives that guide the development of the architectural model in Fig. 1 are the following:

- Personal data must be processed legitimately, confirming judicature to the owner. Therefore, restrictions should apply by the individuals whose personal data processed, such as the terms of usage;
- Data acquisition should be secure along with the flow from the initial phase of the development. For instance, from sensors to the backend repository and IoT devices;
- Interlinked data, becoming beneficial through semantic interrogations. Thus, linking data should be simple and effective between trusted sites;
- Delivering quality digital healthcare services requires the system to be compatible and able to serve multiple operating environments. We aim to implement a system that requires low computational complexity to maintain the advantage of limited calculation time and memory usage;

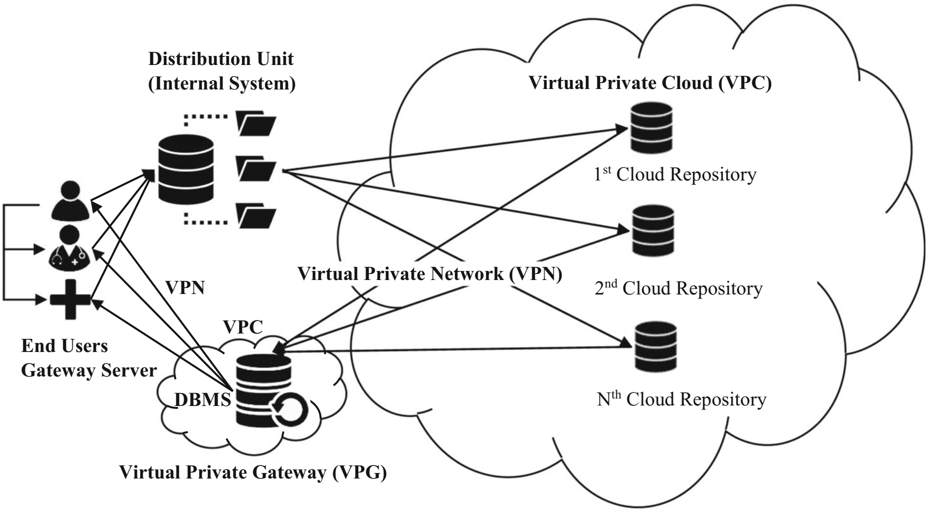

Fig. 1 Architecture of the proposed model

- Government legislation obliges healthcare ecosystems to use secure data management and privacy techniques. The cross-border healthcare data exchange aligned with the country's bioethics legislation that provides the data;
- Since the COVID-19 pandemic, it is a prerequisite for healthcare systems to exchange and share through internet medical records. Thus, the paper aims to provide a novel method for the safe exchange of confidential datasets and medical images.

Initially, we implement a literature review from various scientific articles and books to study the relevant work in this domain and set our innovative contribution. After that, the paper analyses the proposed model's architecture, including the VPN's data flow process. In the same section, we analyze the fragmentation process by applying an example of separating health care data into fragments. Using Newton-Gregory's divided difference interpolation, we implement reconstruction and retrieve a specific health record from the primary dataset. The prerequisite requirement for medical data exchange is medical image transfer. We dedicate a subsection on image secret sharing framework based on the same theory of k out of n secret sharing, including an example. The last section comprises the conclusion and further discussion for future work and contribution in this domain framework.

2 Literature review

Limitation to integrate smart services by connecting heterogeneous platform devices through the IoT because they are prone to hardware/software and network attacks and, if not properly secured, can lead to privacy issues. To resolve the problem, S. Sridhar and S. Smys et al. proposed an Intelligent Security Framework for IoT Devices [30]. Snezana S. et al. introduced a novel concept of personal health records based on an e-health strategy where patients own their data using different ways of obtaining data [29]. The article [3] developed a hybrid measurement technique for digital image watermarking using medical images (X-ray, MRA, and CT), an extremely robust method for protecting clinical information. An innovative watermarking scheme based on the biorthogonal family (biorthogonal 2.2, biorthogonal 3.5, and biorthogonal 5.5) wavelet transform [4]. Simultaneously, it used a convolution for eyelets wavelet transform and conflicts wavelet transform to exchange images in the IoT frame. In the paper [2], the authors proposed a watermarking scheme in the structure of Daubechies wavelets, Daubechies-5, and Daubechies-7 wavelet transform. This wavelet approach is highly robust against various attacks, prohibiting the digital data's piracy and authentication.

Aggarwal et al. have initially proposed the fragmentation cryptographic technique model by dividing the dataset among two data repositories. Although the idea was innovative, the collaboration between the two servers and the restriction of repositories lead to a lack of security and require further encryption to ensure the data's privacy [21]. After that, Ciriani et al. proposed a model without limitations on the number of datasets partitioning based on improved security frame encryption derived from fragments [15, 18]. In 2009 Ciriani et al. proposed a cryptographic fragmentation model where the data owner manages his reliable DBMS [16, 17]. Following Shamir's [28] proposal for a secret sharing scheme, Agrawal et al. and Emekci et al. extended the model by dividing and storing data into CRs, which could only be reconstructed by the knowledge of any k of the n shares and the secret value [1]. The model also reveals information by queries without deciphering the essential attributes of the subsets [19]. Sareen et al. contribute to their work by proposing a new model to protect the confidentiality of outsourced data [27].

Naor and Shamir et al. introduced the idea of image secret sharing by distributing an image into several different images, and the reconstruction is done only by aligning the shares [25]. Based on Naor's and Shamir's secret sharing scheme, which referred to as black and white images, Verheul and Tilborg et al. extended this framework to coloured photos [32]. The same approach of secret image share without the use of cryptography followed by Chin-Chen Chang et al. as well as Ching-Nung Yang et al. [13, 14, 36]. Bisio, I., Fedeli, A., Lavagetto, F. et al. conducted a numerical study dedicated to evaluating the implementation of a microwave imaging method to detect stroke [9]. I. Bisio, C. Garibotto, A. Grattarola, F. Lavagetto and A. Sciarrone et al. introduced the IoT as the key to I4.0 production optimization [10]. I. Bisio, F. Lavagetto, M. Márchese and A. Sciarrone et al. obtainable a performance assessment among AR approaches based on the accelerometer signal recorded through patients' smartphones [8].

In the healthcare industry, some limited caregivers vigorously promote innovative technologies. Based on the above research projects, this paper aims to integrate confidentiality into the exchange of healthcare data provided as a text, either as an image. The novel idea generates a state-of-the-art model based on a fundamental mathematical approach that could be the key to ensuring the digitization of an ecosystem framework for virtual medical therapy and remote treatment. The goal is health data exchange architectures, application interfaces that allow data to be accessed and shared securely and adequately across the spectrum of care, in all applicable settings, and with relevant stakeholders.

3 Proposed model

For prosperous and interoperable data sharing, we proposed the development of data spaces where everyone accepted. Still, the entry should be secure, the management system will identify who uses the system, and all trusted sites will align with the regulations. Figure 1 is a visual presentation of the proposed approach. The raw data generated by sensors applied to users or the data provided by doctors, hospitals, laboratories, etc., will be distributed in fragments based on the owners' requirements and the regulation of restriction concerning the level of confidentiality. In terms of data holder requirements, the distribution unit increases or decreases privacy level to distribute sections to multiple servers and maintain security. Thus, a commitment from the SLA Service Level Agreement will establish appropriate service and confidentiality levels by cloud storage service providers. After that, dataset fragments are distributed in separate cloud data repositories. The original dataset can be reconstructed only from the DBMS and provide data strictly only to certified users.

3.1 Interpretation

Figure 1 shows the end user's gateway server is connected to VPG Virtual Private Gateway in VPC Virtual Private Cloud to establish a VPN Virtual Private Network connection [24]. This scheme provides a connection via a private IP address. It allows the exchange of VPCs in different areas in a public cloud that can connect multiple VPCs within a public cloud for communication without the Internet connection [23]. We propose constraining constraints that will be the rule for distribution among the attributes as agreed through SLA regarding the data owner requirements. If A is a set of users' attributes and c is a set of confidentiality constraints, then c will be a subset of A, $c \subseteq A$ and each constraint cannot be a subset of another constraint [22]. A constraint is defined as the restriction for combining sensitive attributes within the same fragment [5]. The Singleton pattern's deployment will ensure that a dataset has only one acute attribute instance and provides a global access point [7]. The distribution module will manage sharing datasets into separated CR concerning user requirements regarding which attributes agreed in SLA to be together. After that, each CR server module will further distribute the encrypted datasets into cloud repositories. The reconstruction phase will follow the VPN path through the reliable DBMS, which will compute each share, recover, and present the data to the end-users.

3.2 Mathematical approach

Let A be the set of attributes $a_1, a_2, \ldots, a_n$ which the provider requires to distribute among CR and C the set of confidential constraints $c_1, c_2, \ldots, c_n$ where $c_i \subset A$. Constraints separated into singleton where unique sensitive attributes are alone in a set and subset of constraints where the attributes within cannot merge with others. The attributes fragmentation will be applied in the distribution unit by an algorithm based on the decision tree approach. It will calculate the minimum fragmentation that satisfies all confidence-building correlation constraints [18]. Singleton constraints will be distributed from the same unit by a $(k.\ n)$ threshold scheme approach in such a way that the knowledge of any $k \leq n$ sensitive attribute values and the knowledge of the secret x_i, $i \in 1,\ 2\ldots,\ n$ stored in DBMS can retrieve the information, but no group of $k-1$ or fewer can do so even with the knowledge of x_i. By $k-1$ coefficients we mean the set of $\{a_0, a_1, \ldots, a_{k-1}\}$ constants which derives from a_0 the National Identity Number (NIDN) and the respective divided differences as $a_0 = \Delta_{P(x_{k-1})}, a_1 = \Delta^2_{\Delta P(x_{k-1})}, \ldots, a_{k-1} = \Delta^{n-k-1}_{\Delta^{n-k-2} P(x_{k-1})}$. Therefore, if we want to distribute the information into k fragments, then we choose $(k-1)$ randomly coefficients and we let the constant value a_0 be the sensitive value of NIDN, thus creating a $(k-1)$ degree polynomial as follow:

$$P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$$

According to the above, the DBMS stores the secret information $x = (x_1, x_2, \ldots, x_n)$, whereby the knowledge of polynomial coefficients and the substitution of x_i, (the large of i, corresponds to the number of shares) can compute the encrypted values of NIDN National Identity Number from $P(x_i)$, $i = 1, 2, \ldots, k$, and thus by just substituting k of the n values from the vector x. Through Newton-Gregory's divided difference interpolation and by the knowledge of k order pairs $(x_i, P(x_i))$, $i = 1, 2, \ldots, k$ we can determine the $(k-1)$ coefficients of the polynomial as well as the original value of NIDN corresponding to the constant a_0 as follow:

$$P(x) = P(x_{k-1}) + \Delta_{P(x_{k-1})}(x-x_{k-1}) + \Delta^2_{\Delta P(x_{k-1})}(x-x_{k-1})(x-x_k) + \ldots + \Delta^{n-k-1}_{\Delta^{n-k-2}P(x_{k-1})} \prod_{i=k-1}^{n} (x-x_i)$$

Where $\Delta_{P(x_{k-1})}, \Delta^2_{\Delta P(x_{k-1})}, \ldots, \Delta^{n-k-1}_{\Delta^{n-k-2}P(x_{k-1})}$ will be the 1st, 2nd and $(n-k-1)^{th}$ divided differences, respectively.

3.3 Paradigm

Let A be the set of patients' attributes that includes the following information to be distributed among CR:

A = {National Identity Number (NIDN), Name, Date of Birth (DoB), Mobile Number (MN), Postal Code (PC), Chronic Disease (CD)}

c_0= {NIDN} (sensitive information)

c_1= {Name, DoB}
c_2= {Name, MN}
c_3= {Name, PC}
c_4= {Name, CD}

Names in association with any other attribute considered as a sensitive information

c_5= {DoB, MN, PC}
c_6= {DoB, MN, CD}

Date of birth in cooperation with mobile number can infer the identity of users and in association with other attributes is consider sensitive

By fragmentation, we mean the distribution of attributes so that their associated values are separated and linked only to the encryption key. An example of fragmenting the attributes involved in the constraints so that they are not visible together could be $f_1 = \{Name\}$, $f_2 = \{DoB, MN\}$ and $f_3 = \{PC, CD\}$. Fragments are stored in three separate CR CR1, CR2, and CR3, respectively. We will develop a second-degree polynomial to share the data among CRs as follow:

$$P(x) = a_2x^2 + a_1x + a_0$$

Where a_0 represents the NIDN and the coefficients $a_1 = (1,2,5,6,4)$ and $a_2 = (7,3,2,1,9)$ randomly selected. Also, the secret values of x_i, $i = 1, 2, 3$ are randomly selected and correspond to each SP respectively, let $x_1 = 1, x_2 = 2, x_3 = 4$. Tables 1, 2, 3, 4 and 5 presents the computational results of substitution for each polynomial of the coefficients and the secret values.

Table 1 Registered data

NIDN	Name	DoB	MN	PC	CD
880,618	Andrew	26/03/1984	96,536,499	4529	Cancer
526,548	Nicolas	12/05/1968	99,652,342	2324	Diabetes
616,636	Jane	13/07/1975	96,521,548	2528	Heart disease
844,131	David	25/04/1983	99,215,482	4528	Asthma
321,131	Mathew	01/09/1950	99,992,272	5232	Epilepsy

The fragments will distribute as shown within the following tables, presenting an incorrect value of NIDN for each data from Table 2:

Reconstruction implementation can only be done by the knowledge of the three ordered pairs $\{(x_i, P(x_i)), i = 1, 2, 3\}$ corresponding to the three CRs which kept stored in DBMS. The decryption implemented using Newton-Gregory's divided difference interpolation, as shown in Table 6, which will reconstruct the polynomial and reveal the original value of NIDN as the constant part of it a_0 [27].

The calculations resulting from Table 6 shown below:

$$\begin{aligned}
P(x) &= P(x_2) + \Delta_{P(x_2)}(x-x_2) + \Delta^2_{\Delta P(x_2)}(x-x_2)(x-x_3)\\
P(x) &= 880636 + 13(x-2) + 1(x-2)(x-4)\\
P(x) &= 880636 + 13x-26 + x^2-4x-2x + 8\\
P(x) &= x^2 + 7x + 880618
\end{aligned}$$

After computing the constant value a_0 that reveals the initial NIDN number. As shown in Table 7, we can retrieve any information from the patient's record.

4 Image exchange

A visual secret sharing scheme is a method of sharing intimate images among a group of stakeholders. Each participant gets a piece of the secret image, called a share. The allowed coalition of the participators can reveal the original image by accumulating their shares. However, any subsets of the alliance cannot retrieve the secret image by amassing their shares. For instance, if we called each share, transparency, the secret is visible in a (k, n) visual cryptography scheme if ≥ k transparencies stack together.

Nevertheless, none can see the original image if <k transparencies are stacked together. Transmitting and sharing information in a healthcare system requires medical image sharing (e.g., MRI images). Thus, we propose a secure fragmentation scheme for image exchange in

Table 2 Substitution results

NIDN	Polynomial P(x)	$x=1$ CR_1	$x=2$ CR_2	$x=4$ CR_3
880,618	$1\times{}^{2}+7x+880{,}618$	880,626	880,636	880,662
526,548	$2\times{}^{2}+3x+526{,}548$	526,553	526,562	526,592
616,636	$5\times{}^{2}+2x+616{,}636$	616,643	616,660	616,724
844,131	$6\times{}^{2}+1x+844{,}131$	844,138	844,157	844,231
321,131	$4\times{}^{2}+9x+321{,}131$	321,144	321,165	321,231

Table 3 Data of CR1

NIDN	Name
880,626	Andrew
526,553	Nicolas
616,643	Jane
844,138	David
321,144	Mathew

the same concept of k out of n secret sharing. We have incorporated a visual secret sharing scheme to encode an image required to be secure in "shadow" embodiments called shares. The secret can be visually reconstructed only when k or more shares are available. Each pixel of the secret image is "expanded" into m sub-pixels in each share, and in the reconstruction process, the stacking of the sub-pixels is a Boolean 'OR' operation.

4.1 Implementation

The method requires distributing the image's pixels in n modified versions and sharing them among n cloud repositories through VPN. Each fragment is a collection of m subpixels. It is essential for logic disciplines, including cryptography, to use a fundamental rule named Richard Hamming and Hamming Weight. The determination comes from the count of '1' within a binary number. For instance, the Hamming Weight for 101,001 is 3, and 1,110,011 is 5. Hence the architecture is represented by $n \times m$ Boolean matrix $A = [A_{ij}]$, where $a_{ij} = 1$ if the j$^{\text{th}}$ subpixel in the i$^{\text{th}}$ share is black; otherwise, it is 0, represented by white. Grey-scale on images revealed using the Hamming weight defined as the amount of '1' from the 'OR' operation on matrix A [34]. More specifically, $B = \text{OR}(i_1, i_2, \ldots, i_r)$ where $i_1, i_2, \ldots, i_r$ are the rows of matrix A and $H(B)$ is the Hamming weight. C_0 and C_1 are defined as the $n \times m$ Boolean matrices that can compute the k out of n secret sharing. White and black pixel corresponds to the two matrices respectively, which specify the m-subpixels' colour among the n shares in n repositories. The requirements for a calculation to be considered valid are the following:

1. For any $A \subseteq C_0$ the B^0 among k out of the n rows satisfies $H(B^0) \leq l,\ l \in \mathbb{Z}^+$
2. For any $A \subseteq C_1$ the B^1 among k out of the n rows satisfies $H(B^1) \leq h,\ l \in \mathbb{Z}^+,\ l < h \leq m$
3. For any $\{i_1, i_2, \ldots, i_q\} \subseteq \{i_1, i_2, \ldots, i_n\}$, $q < k$ the $q \times m$ matrices D_t, $t \in \{0, 1\}$ derive by restricting each C_t to rows $i_1, i_2, \ldots, i_q$ cannot be distinguished

The definition of contrast, which is the combination of the Hamming Weight difference between white and black pixels in a share, could be calculated as follows:

Table 4 Data of CR2

NIDN	DoB	MN
880,636	26/03/1984	96,536,499
526,562	12/05/1968	99,652,342
616,660	13/07/1975	96,521,548
844,157	25/04/1983	99,215,482
321,165	01/09/1950	99,992,272

Table 5 Data of CR3

NIDN	PC	CD
880,662	4529	Cancer
526,592	2324	Diabetes
616,724	2528	Heart disease
844,231	4528	Asthma
321,231	5232	Epilepsy

$$a = \frac{H\left(B^1\right) - H\left(B^0\right)}{m} = \frac{h - l}{m}$$

Let P_0 and P_1 be the probability of white and black pixel appearing in a white and black area respectively, and let $P_{th} \in [0, 1]$ be a threshold probability. If $P_0 \geq P_{th}$ and $P_1 \leq P_{th} - a$ where $a \geq 0$ is the contrast as defined above, then the frequency of white pixels in a white area of the recovered image will be higher than in a black area. E_0 and E_1 are white and black sets respectively with n_λ and n_γ ($n \times 1$, matrices). The reconstruction probability is valid if the following conditions are met [35]:

1. The 'OR' operation of any $n \times 1$ matrix is $H(B)$
2. If P_0 and P_1 are the probabilities of white ($white = 0$) appearing in the sets λ and γ respectively, then we have the satisfaction of $P_0 \geq P_{th}$ and $P_1 \leq P_{th} - a$
3. For any $\{i_1, i_2, \ldots, i_q\} \subseteq \{i_1, i_2, \ldots, i_n\}$, $q < k$, $P_0 = P_1$

The probabilities P_0 and P_1 are calculated as follow:

$$P_0 = \frac{m - l}{m}, P_1 = \frac{m - h}{m}$$

Let $G^i = A^0 \circ \ldots \circ A^0 A^1 \circ \ldots \circ A^1$, $i = 0, \ldots, g - 1$, where $g \geq 2$ collections of G^i matrices develop a secret sharing scheme for g grey-levels with pixel expansion defined by m_g. Reconstruction applied with $a^{(1,0)}, \ldots, a^{(g-1,g-2)}$ representing contrast and $\{d_i\}$, $i = 0, \ldots, g - 2$ the threshold sets for $n \times m_g$, G_i matrices if the following two conditions met:

1. $H(B^i) \leq d_i - a^{(i+1,i)}$, where for G^{i+1} the Hamming weight for the 'OR' operation of any k of n rows results that $H(B^{i+1}) \geq d_i$

Table 6 Newton-Gregory's divided difference interpolation

i	x_i	$P(x_i)$	$\Delta_{P(x_i)}$	$\Delta^2_{\Delta P(x_i)}$
1	1	880,626		
			$\frac{P(x_2) - P(x_1)}{x_2 - x_1} = 10$	
2	2	880,636		$\frac{\Delta_{P(x_2)} - \Delta_{P(x_1)}}{x_3 - x_1} = 1$
			$\frac{P(x_3) - P(x_2)}{x_3 - x_2} = 13$	
3	4	880,662		

Table 7 Reconstructed table

NIDN	Name	DoB	MN	PC	CD
880,618	Andrew	26/03/1984	96,536,499	4529	Cancer

2. For any $\{r_1, r_2, \dots, r_j\} \subseteq \{1, \dots, k\}$, $1 \le j < k$, the matrices obtained by restricting $G^i_{j \times m_g}$ to rows r_1, r_2, …, r_j are equal up to a column permutation.

The following equation calculates contrast:

$$a^{(i+1,i)} = \frac{H(B^{i+1}) - H(B^i)}{m_g} = \frac{a_{i+1} - a_i}{m_g} = \frac{h - l}{(g-1) \times m} = \frac{a}{g-1}, i = 0, \dots, g-2$$

If a_i is the amount of '1' in G^i and b_i the amount of '0' then $a_i = H(B^i) = l \times (g - i - 1) + h \times i$ and $b_i = m_g - a_i = (m - l) \times (g - i - 1) + (m - h) \times i \Longrightarrow a_i + b_i = m \times (g - 1) = m_g$ [12].

After that, we select $s = 1, \dots, m_g$ random columns from G^i matrices and obtain $\binom{m_g}{s}$ the $n \times s$ matrices $T_s^{(i)} = \left\{ G^i\big|_{s,p} \right\}, p = 1, \dots, \binom{m_g}{s}$. The average Hamming weight of the i^{th} grey-level reconstructed pixel is $\overline{H_s^i} = \sum_{j=0}^{s} j.p_{s,j}^{(i.)}$and $p_{s,j}^{(i)}$ defined as the probabilistic of the Hamming weight of the 'OR' operation of any k rows, which is $j = 0, \dots, s$. The average grey-level and average contrast, respectively, are calculated as follow:

$$\overline{e_s^{(i)}} = \frac{\overline{H_s^i}}{S}$$
$$\overline{a_s^{(i+1,i)}} = \overline{e_s^{(i+1)}} - \overline{e_s^{(i)}}, i = 0, \dots, g-2$$

Thus, the grey level $i = 0, 1, \dots, g - 1$ is constructed by the $\binom{m_g}{s}$, $n \times s$, $G^i|_{s,\,p}$ matrices respectively, where $p = 1, \dots, \binom{m_g}{s}$ and the set $T_s^{(i)} = \left\{ G^i\big|_{s,p} \right\}$ can be used to construct a grey-scale probabilistic visual secret sharing scheme.

4.2 Paradigm

Let $A^0 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$ and $A^1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be the two fundamental Boolean matrices for a black and white pixel respectively the 'OR' operation (the operator 'OR' gives 1 as a result if at least one of the two elements is 1) of the elements in any two rows of A^0 gives as a result of two zeros, thus $h = 2$ and respectively for the same reason from A_1 derives $l = 1$. Therefore, we assume that the contrast of results, which is also known as the relative difference between the black and white pixel reconstruction, is $= \frac{h-l}{m} = \frac{1}{3}$.

From the definition of E_0 and E_1 we have $E_0 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}$ and $E_1 = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$ and as mentioned λ and γ calculated by the 'OR' operation of the column vectors, so $\lambda = \left\{ H\left(\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right), H\left(\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right), H\left(\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right) \right\} = \{0,\ 0,\ 1\}$ and $\gamma = \left\{ H\left(\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right), H\left(\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right), H\left(\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right) \right\} = \{1,\ 1,\ 1\}$. Thus, the appearance probabilities of white colour are $P_0 = \frac{m-l}{m} = \frac{3-1}{3} = \frac{2}{3}$, $P_1 = \frac{m-h}{m} = \frac{3-2}{3} = \frac{1}{3}$ and the threshold probability $P_{th} = \frac{2}{3}$, since the contrast was $\alpha = \frac{1}{3}$ the second condition was met. The last requirement referring to the equality of the two probabilities fulfilled as for all the shadows $\lambda = \{H([0]), H([0]), H([1])\} = \{0,\ 0,\ 1\}$ and $\gamma = \{H([1]), H([0]), H([0])\} = \{1,\ 0,\ 0\}$, $\gamma = \{H([0]), H([1]), H([0])\} = \{0,\ 1,\ 0\}$ and $\gamma = \{H([0]), H([0]), H([1])\} = \{0,\ 0,\ 1\}$ for shadows 1,2 and 3 respectively, so $P_0 = P_1 = \frac{2}{3}$.

$$G^0 = A^0 \circ A^0 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$G^1 = A^0 \circ A^1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$G^2 = A^1 \circ A^1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

The pixel expansion is $m_g = (g-1) \times m = 6$ and the contrasts computed as $a^{(1,0)} = \frac{H(B^1)-H(B^0)}{m_g} = \frac{3-2}{6} = \frac{1}{6}$, $a^{(2,1)} = \frac{H(B^2)-H(B^1)}{m_g} = \frac{4-3}{6} = \frac{1}{6} \Rightarrow a^{(1,0)} = a^{(2,1)}$

$$T_5^{(0)} = \left\{ \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \right\}$$

$$T_5^{(1)} = \left\{ \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \right\}$$

$$T_5^{(2)} = \left\{ \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \right\}$$

The 'OR' operation of the q_1th row and the q_2th row of the set $T_5^{(0)}$ are $j \in \{0, 1, 2, 3, 4, 5\}$. The data included in the first row of Table 8 calculated as follow:

$$p_{5,0}^{(0)} = p_{5,3}^{(0)} = p_{5,4}^{(0)} = p_{5,5}^{(0)} = 0/6 = 0, p_{5,1}^{(0)} = 2/6 = 1/3, p_{5,2}^{(0)} = 4/6 = 2/3$$

$$\overline{e_s^{(i)}} = \frac{H_s^i}{S} = \frac{1}{s} \sum_{j=0}^{s} j.p_{s,j}^{(i)} \Rightarrow \overline{e_5^{(0)}} = \frac{1}{5} \sum_{j=0}^{5} j.p_{5,j}^{(0)} = \frac{1}{5}\left(1.\frac{1}{3} + 2.\frac{2}{3}\right) = \frac{1}{3}$$

Table 8 Values of average grey-levels of probabilistic scheme

$p_{5,j}^{(i)}$	$j=0$	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$	$\overline{e_5^{(i)}}$
$I=1$	0	1/3	2/3	0	0	0	1/3
$I=2$	0	0	1/2	1/2	0	0	1/2
$I=3$	0	0	0	2/3	1/3	0	2/3

Table 9 contains data of $p_{s,j}^{(i)}$ and $\overline{e_s^{(i)}}$ in which $s = 1, 2, 3, 4, 5, 6$ and $i = 1, 2, 3$ from where derives that $\overline{a}^{(1,0)} = \overline{a}^{(2,1)} = 1/6$.

5 Conclusions & future work

Sharing data over the cloud requires confidentiality, privacy, control, and compliance with laws and regulations. Thus, our approach suggested a framework that presents secure encryption of data stored in cloud repositories. Encryption based on an innovative data set fragmentation technique uses CRs through VPN to distribute data to separate sensitive data securely. In the future, we introduce a mathematical approach to Newton-Gregory interpolation to retrieve

Table 9 Data for $p_{s,j}$ and e_s

	$j=0$	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$	$j=6$	$\overline{e_s^{(0,1,2)}}$
For $i=1, 2, 3$								
$p_{1,j}^{(1)}$	2/3	1/3	–	–	–	–	–	1/3
$p_{2,j}^{(1)}$	6/15	8/15	1/15	–	–	–	–	1/3
$p_{3,j}^{(1)}$	1/5	3/5	1/5	0	–	–	–	1/3
$p_{4,j}^{(1)}$	1/15	8/15	6/15	0	0	–	–	1/3
$p_{5,j}^{(1)}$	0	1/3	2/3	0	0	0	–	1/3
$p_{6,j}^{(1)}$	0	0	1	0	0	0	0	1/3
$p_{1,j}^{(2)}$	1/2	1/2	–	–	–	–	–	1/2
$p_{2,j}^{(2)}$	3/15	9/15	3/15	–	–	–	–	1/2
$p_{3,j}^{(2)}$	1/20	9/20	9/20	1/20	–	–	–	1/2
$p_{4,j}^{(2)}$	0	1/5	3/5	1/5	0	–	–	1/2
$p_{5,j}^{(2)}$	0	0	1/2	1/2	0	0	–	1/2
$p_{6,j}^{(2)}$	0	0	0	1	0	0	0	1/2
$p_{1,j}^{(3)}$	1/3	2/3	–	–	–	–	–	2/3
$p_{2,j}^{(3)}$	1/15	8/15	6/15	–	–	–	–	2/3
$p_{3,j}^{(3)}$	0	1/5	3/5	1/5	–	–	–	2/3
$p_{4,j}^{(3)}$	0	0	6/15	8/15	1/15	–	–	2/3
$p_{5,j}^{(3)}$	0	0	0	2/3	1/3	0	–	2/3
$p_{6,j}^{(3)}$	0	0	0	0	1	0	0	2/3

and reconstruct original data. A detailed example using random data explains the fragmentation data distribution and then the reconstruction application to retrieve a specific record. Fragmentation further improves current data encryption approaches by reducing the burden of high computing on the server. As shown, it can effectively apply to images to avoid cryptographic calculations and be used to transfer confidential images through the cloud. Therefore, we have proposed a binary secret sharing solution for grayscale images to be used in healthcare for a completely secure data exchange framework.

Integrating edge computing with cloud computing requires an efficient and secure data exchange during data flow and secure cloud repositories. Also, big data growth increases the obligations to secure information from data breaches and leakages of information. Therefore, we aim to continue contributing to data privacy mechanisms on big data to protect healthcare data exchange and storage confidentiality in future work. The data-rich environments resulting from cloud computing's radical innovation in collaboration with ML Machine Learning and AI Artificial Intelligence require advanced encryption and security techniques with a low computational load. A cypher approach that satisfies the fundamental security properties of image could be used in conjunction with fragment images for further data exchange safety.

Acknowledgements The research work presented in this article was partially supported by the project entitled 'Smart and Health Ageing through People Engaging in supporting Systems' with acronym SHAPES, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857159. Undertaken by the SPHINX project through the European Union's Horizon 2020 Research and Innovation Programme (Digital Society, Trust & Cyber Security E-Health, Well-Being and Ageing) under grant agreement 826183. It is also part of the Ambient Assisted Living (AAL) project vINCI: "Clinically-validated INtegrated Support for Assistive Care and Lifestyle Improvement: The Human Link" funded by Research & Innovation Foundation in Cyprus under the AAL framework with Grant Nr. vINCI /P2P/AAL/0217/0016.

We sincerely thank anonymous reviewers for critically reading the manuscript and suggesting substantial improvements, which helped us significantly improve our paper's presentation and research work quality.

References

1. Agrawal D, Abbadi AE, Emekci F, Metwally A (2009) Database management as a service: challenges and opportunities, in 2009 IEEE 25th International Conference on Data Engineering, Shanghai
2. Alshayea T, Mavromoustakis C, Mastorakis G, Batalla JM, Markakis E, Pallis E (2018) On the Efficiency evaluation of a novel scheme based on daubechies wavelet for watermarking in 5G," in 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona
3. Alshayeh T, Mavromoustakis C, Batalla JM, Mastorakis G (Dec. 2019) A hybridized measurement methodology for different wavelet transformations targeting medical images in internet of things (IoT) infrastructures. Measurement 148(106813)
4. Alshayeh T, Mavromoustakis C, Batalla JM, Mastorakis G, Mukherjee M, Chatzimisios P (2019) Efficiency-aware watermarking using different wavelet families for the internet of things, in 2019 IEEE International Conference on Communications (ICC), Shanghai
5. Anderson S, Revesz P (2007) CDB-PV: a constraint database-based program Verifier, in International Symposium on Abstraction, Reformulation, and Approximation
6. Andreas A, Mavromoustakis C, Mastorakis G, Mumtaz S, Batalla JM, Pallis E (2020) Modified machine learning Techique for curve fitting on regression models for COVID-19 projections. In: IEEE international workshop on computer aided modeling and Design of Communication Links and Networks (CAMAD)
7. Barták R (2007) Generating implied boolean constraints via singleton consistency, in International Symposium on Abstraction, Reformulation, and Approximation

8. Bisio I, Lavagetto F, Márchese M, Sciarrone A (2014) Comparison of situation awareness algorithms for remote health monitoring with smartphones, in 2014 IEEE Global Communications Conference, Austin
9. Bisio I, Fedeli A, Lavagetto F, Pastorino M, Randazzo A, Sciarrone A, Tavanti E (27 Jun. 2017) A numerical study concerning brain stroke detection by microwave imaging systems. Multimed Tools Appl 77:9341–9363
10. Bisio I, Garibotto C, Grattarola A, Lavagetto F, Sciarrone A (2018) Exploiting context-aware capabilities over the internet of things for industry 4.0 applications. IEEE Netw 32(3):101–107, May/June
11. Blumenthal D, Tavenner M (05 Aug. 2010) The "meaningful use" regulation for electronic health records. N Engl J Med 363:501–504
12. Blundo C, Santis AD, Naor M (30 Nov. 2000) Visual cryptography for grey level images. Inf Process Lett 75(6):255–259
13. Chang C-C, Yu T-X (2002) Sharing a secret gray image in multiple images, in First International Symposium on Cyber Worlds, Tokyo, Japan
14. Chang C-C, Tsai C-S, Chen T-S (2000) A new scheme for sharing secret color images in computer network, in Seventh International Conference on Parallel and Distributed Systems, Iwate, Japan
15. Ciriani V, Vimercati SDCd, Foresti S, Jajodia S, Paraboschi S, Samarati P (2007) Fragmentation and encryption to enforce privacy in data storage, in 12th European Symposium On Research In Computer Security
16. Ciriani V, Vimercati SDCd, Foresti S, Jajodia S, Paraboschi S, Samarati P (2009) Keep a few: outsourcing data while maintaining confidentiality, in European Symposium on Research in Computer Security
17. Ciriani V, Vimercati SDCd, Foresti S, Jajodia S, Paraboschi S, Samarati P(2009) Enforcing confidentiality constraints on sensitive databases with lightweight trusted clients, in IFIP Annual Conference on Data and Applications Security and Privacy
18. Ciriani V, Vimercati SDCD, Foresti S, Jajodia S, Paraboschi S, Samarati P (July 2010) Combining fragmentation and encryption to protect privacy in data storage. ACM Trans Inf Syst Secur 13(3):1–33
19. Emekci F, Methwally A, Agrawal D, Abbadi AE (01 Apr 2014) Dividing secrets to secure data outsourcing. Inf Sci 263:198–210
20. "enovacom," Enovacom Canada Inc., [Online]. Available: https://www.enovacom.com/interoperability/fhir-what-are-the-challenges-to-adoption/.
21. Gagan A, Mayank B, Prasanna G, Hector GM, Krishnaram K, Rajeev M, Utkarsh S, Dilys T, Ying X (2005) Two can keep a secret: a distributed architecture for secure database services, in The Second Biennial Conference on Innovative Data Systems Research (CIDR 2005), Asilomar, California
22. Le DN, Seth B, Dalal S (12 Sep. 2018) A hybrid approach of secret sharing with fragmentation and encryption in cloud environment for securing outsourced medical database: a revolutionary approach. J Cyber Secur Mobility 7(4):379–408
23. Leng C, Yu H, Wang J, Huang J (Apr. 2013) Securing personal health Records in the Cloud by enforcing sticky policies. TELKOMNIKA 11(4):2200–2208
24. Mavromoustakis C, Batalla JM, Mastorakis G, Markakis E, Pallis E (Jul. 2018) Socially oriented edge computing for energy awareness in IoT architectures. IEEE Commun Mag 56(7):139–145
25. Naor M, Shamir A (1994) Visual cryptography. Advances in Cryptology, EUROCRYPT 950:1–12
26. Odisho A, Lui H, Yerramsetty R, Bautista F, Gleason N, Martin E, Young J, Blum M, Neinstein A (2020) Design and development of referrals automation, a SMART on FHIR solution to improve patient access to specialty care. JAMIA Open 3(3):405–412
27. Sareen S, Sood S, Gupta SK (06 Feb. 2016) Towards the design of a secure data outsourcing using fragmentation and secret sharing scheme. Inform Secur J A Global Perspective 25(1–3):39–53
28. Shamir A (Nov 1979) How to share a secret. Commun ACM 22(11)
29. Snezana S, Kilintzis V, Jakimovski B, Jolevski I, Beredimas N, Mourouzis A, Corbev I, Chouvarda I, Maglaveras N, Trajkovik V (2020) Cloud based personal health records data exchange in the age of IoT: The Cross4all Project," in Machine Learning and Applications. ICT Innovations 2020. Communications in Computer and Information Science, vol. 1316, Springer, Cham, pp. 28–41.
30. Sridhar S, Smys S (2017) Intelligent security framework for iot devices cryptography based end-to-end security architecture, in International Conference on Inventive Systems and Control , Coimbatore
31. Stoldt J-P, Weber J (2020) Safety Improvement for SMART on FHIR Apps with Data Quality by Contract," in IEEE International Conference on Software Architecture Companion , Salvador, Brazil
32. Verheul E, Tilborg H (1997) Constructions and properties of k out of n visual secret sharing schemes. Des Codes Crypt 11:179–196
33. WH Organization, 2020-2024. [Online]. Available: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_42.
34. Wang D, Yi F, Li X (01 June 2011) Probabilistic visual secret sharing schemes for grey-scale images and color images. Inf Sci 181(11):2189–2208

35. Yang C-N (Mar. 2004) New visual secret sharing schemes using probabilistic method. Pattern Recogn Lett 25(4):481–494

36. Yang C-N, Laih C-S (2000) New colored visual secret sharing schemes. Des Codes Crypt 20:325–336

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Affiliations

Andreou Andreas[1] · **Constandinos X. Mavromoustakis**[1] · **George Mastorakis**[2] · **Dinh-Thuan Do**[3] · **Jordi Mongay Batalla**[4] · **Evangelos Pallis**[5] · **Evangelos K. Markakis**[5]

Constandinos X. Mavromoustakis
mavromoustakis.c@unic.ac.cy

George Mastorakis
gmastorakis@hmu.gr

Dinh-Thuan Do
dodinhthuan@iuh.edu.vn

Jordi Mongay Batalla
jordi.mongay.batalla@pw.edu.pl

Evangelos Pallis
pallis@hmu.gr

Evangelos K. Markakis
markakis@pasiphae.eu

[1] Department of Computer Science Mobile Systems Laboratory (MoSys Lab), University of Nicosia and University of Nicosia Research Foundation, Nicosia, Cyprus

[2] Department of Management Science and Technology, Hellenic Mediterranean University, 72100 Agios Nikolaos, Crete, Greece

[3] Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh City, Vietnam

[4] Warsaw University of Technology, Warsaw, Poland

[5] Department of Electrical and Computer Engineering, Hellenic Mediterranean University, Heraklion, Crete, Greece