様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　６ 月 ２４ 日現在

機関番号：２１６０２
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ００００２０

研究課題名（和文）秘密分散法の最適性および存在性に関する研究

研究課題名（英文）Study on the existence and the optimality of secret sharing schemes

研究代表者
渡辺　曜大（Watanabe, Yodai）

会津大学・コンピュータ理工学部・上級准教授

研究者番号：７０３６０６７５

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：秘密分散法とは，資格を有する参加者集合のみが復元できるように秘密情報を分散暗号化するための暗号技術であり，重要な情報に対する安全なアクセス制御を実現するための核となる技術です．本研究では，人間の目や耳を用いて復号演算を実行することのできる一風変わった秘密分散法について，いくつかの具体的な構成法を与え，その存在性を確認しました．また，与えた構成法の特性を評価し，その最適性や既存の構成法と比較した特徴について調べました．

研究成果の学術的意義や社会的意義
本研究の学術的な意義として，複数画像を暗号化する人間の目を用いて復号可能な秘密分散法に関しては，(1)最も一般的なアクセス構造を実現する構成法を与えてアクセス制御の適用範囲を最大化したこと，(2)ある構成法が最適でないことを示す簡単な方法を例示したこと，また，音声情報を暗号化する人間の耳を用いて復号可能な秘密分散法に関しては，(3)その定式化を与え，それをみたす構成法が実際に存在することを示したこと，が挙げられます．

研究成果の概要（英文）：The secret sharing scheme is a cryptosystem which encrypts a secret into multiple pieces, called shares, so that only qualified combination of shares can be employed to recover the secret. There exist curious secret sharing schemes whose decryption can be performed by a human. In this study, several constructions of such curious secret sharing schemes were provided, and their performance was examined and compared with that of the existing ones.

研究分野：暗号

キーワード：暗号　秘密分散

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

秘密分散法とは，以下の 2 つの条件をみたすように秘密情報を暗号化して複数の参加者に分配する暗号技術である：(1) 資格を有する参加者集合（有資格集合）は秘密情報を完全に復元できるが，(2) 資格のない参加者集合（禁止集合）は秘密情報に関するいかなる部分情報も得ることができない．秘密情報が分散暗号化され，各参加者に分配される情報のことを分散情報と呼ぶ．秘密分散法の典型的な例は，参加者 n 人のうち k 人以上からなる集合が有資格集合，$k-1$ 人以下からなる集合が禁止集合となるもので，(k,n)-しきい値型秘密分散法とよばれる．適切に設計された秘密分散法は，情報の漏えいと紛失を同時に防ぐことが可能であり，重要な情報に対するアクセス制御を実現するための核となる技術である．

２．研究の目的

秘密分散法に関する重要な未解決問題として，情報比（暗号化された情報のサイズを元の秘密情報のサイズで割ったもの）の最適性の問題，および，計算量的秘密分散法の存在性の問題が挙げられる．これらの問題は，単に実用上重要なだけでなく，例えば，ある特別な計算量的秘密分散法の存在が暗号学におけるもっとも主要な未解決問題の一つを解決することが知られており，学術の立場からも重要である．本研究の目的は，これらの重要な未解決問題を念頭に，秘密分散法の最適性および存在性に関して新しい知見を得ることである．

３．研究の方法

秘密分散法には，人間の目あるいは耳を使って復号が可能な一風変わったものが存在する．前者を視覚復号型秘密分散法，後者を聴覚復号型秘密分散法とよぶ．視覚復号型秘密分散法では，秘密情報（白黒画像）を暗号化して生成された白黒画像を透明なシートに印刷したものが各参加者に分配される分散情報になる．復号は参加者が持ち寄った透明なシート（分散画像）を重ね合わせ，現れた画像を人間の目で判別することにより行われる．一方，聴覚復号型秘密分散法では，分散情報は音声であり，復号は参加者が持ち寄った音声を同時再生し，合成された音声を人間の耳で判別することにより行われる．上述の重要な未解決問題に対して完全な解答を与えることは難問であるため，本研究ではまず，具体的な秘密分散法としてこの視覚復号型秘密分散法および聴覚復号型秘密分散法を取り上げ，その存在性および最適性に関して新しい知見を得ることを目指す．

４．研究成果

(1) 複数画像を暗号化する視覚復号型秘密分散法[1]

複数画像を暗号化する視覚復号型秘密分散法[a][c][h]に関しては，先行研究[g]においてアクセス構造を最も一般的な形に拡張し，それを実現する視覚復号型秘密分散法の構成法を与えているが，この構成法を以下のようにさらに一般化した．まず，視覚復号型秘密分散法の暗号化は，行が参加者，列が分散画素に対応する 2 値行列（に値を持つ確率変数）により表すことができることに注意しておく．ここで，上記構成法で用いられる暗号化関数が，各秘密画像に対応する暗号化関数集合の連結（のランダム列置換）で与えられ，さらにこの関数集合の各関数が，(i) 対応する秘密画像のアクセス構造を実現する視覚復号型秘密分散法を与え，(ii) 他の秘密画像に対応する分散情報の復号に干渉しない，という 2 つの条件をみたすことが本質的であることに注目する．この 2 つの条件(i)，(ii)を，暗号化関数集合の「適合性」とよぶことにする．この適合性をもつ関数集合の連結（のランダム列置換）を暗号化関数とする視覚復号型秘密分散法の構成法を与え，それが実際に最も一般化されたアクセス構造を実現することを示した．さらに，ここで与えた構成法が上述の先行研究で与えられる構成法よりも真に「良い」ことを，前者が後者よりも真に良い特性をもつ（具体的には，情報比が真に小さくなる）視覚復号型秘密分散法を与えるアクセス構造の例を与えることによって示した．

これら 2 つの構成法は，それぞれ他方に対して利点を持っている．すなわち，上述の通り一方は他方よりも真に優れた特性（情報比）をもつ視覚復号型秘密分散法を生成可能であるのに対し，他方は容易に実装可能である．以下，前者を特性指向構成法，後者を実装指向構成法と呼ぶことにする．これら 2 つの構成法に関して，以下の結果を得た．(i) しきい値型複数秘密画像視覚暗号方式[h]と実装指向構成法の画素拡大度を比較し，これらが一致することを確認した．ここで，しきい値型複数秘密画像視覚暗号方式はしきい値型のアクセス構造にのみ適用可能であるのに対し，実装指向構成法は任意のアクセス構造に適用可能であることに注意しておく．つまり，後者は，特性を低下させることなく前者よりも適用範囲を（最大限に）広げることに成功していることになる．(ii) 複数画像を暗号化する視覚復号型秘密分散法の最適性を，単一画像を暗号化する視覚復号型秘密分散法の最適性に帰着させることにより，特性指向構成法であっても最適な視覚復号型秘密分散法を生成できないアクセス構造が存在することを示した．

(2) 音声情報を暗号化する聴覚復号型秘密分散法[2][3]

視覚復号型秘密分散法において秘密情報は画像情報であるが，聴覚復号型秘密分散法には，何を秘密情報とするかに応じて以下の 2 つのタイプが存在する：(i) 2 進文字列を暗号化す

る聴覚復号型秘密分散法[b]，(ii) 音声情報を暗号化する聴覚復号型秘密分散法[i]．ここで，後者においては，秘密音声（の振幅）は有界であるべきであるが復号演算（実数もしくは整数上の足し算）が有界な実数もしくは整数の集合上で閉じていないため，秘密情報と分散情報とは完全に独立にはなりえない．したがって，その安全性を正しく評価することが必要となる．そこで，任意の自然数 n に対して，音声情報を暗号化する (n,n)-しきい値型聴覚復号型秘密分散法の構成法を与え，その安全性を評価した．この結果と，(n,n)-しきい値型視覚復号型秘密分散法に関してすでに知られている結果[e]とを比較し，それぞれの特徴を明らかにした．さらにこれを一般のしきい値型に拡張するために，復号関数を単なる分散音声の和から重み付きの和に一般化した．この一般化に基づいて，(k,n)-しきい値型聴覚復号型秘密分散法の構成法を与え，その安全性を評価した．なお，上述のように復号関数を重み付きの和としたため，復号された秘密音声の品質についても考慮する必要がある．そこで，復号された秘密音声における信号雑音比と暗号化関数のパラメータとの関係を調べた．また，音声情報を暗号化する聴覚復号型秘密分散法の安全性を，実際の秘密音声を用いた計算機実験により評価し，これを理論の結果と比較した．

(3) 構造的類似性(SSIM) 指数の修正およびその視覚復号型秘密分散法への応用[4]
視覚復号型秘密分散法の 2 値（白黒）秘密画像を多値（グレースケール）画像に拡張する一つの方法は，暗号化にデジタルハーフトーニングを利用することである[j]．しかし，複雑なアクセス制御を実現する視覚復号型秘密分散法では，復元された秘密画像のコントラストは必然的に低くなるため，標準的なデジタルハーフトーニングを適用して生成された分散画像から復元された秘密画像を認識することは一般に容易ではない．ここで，復元画像の視覚品質を改善するためには，エッジ構造のような人間の視覚系が敏感である構造情報を強調することが有効である[d]．そこで，構造的類似性(SSIM) 指数を修正して，構造的類似性と色調的類似性の両方を同時に評価できるような指数を構成した．修正された指数の計算コストは SSIM 指数と同程度であるため，これを使用することで既存の最適化に基づくハーフトーニング[f]における目的関数を簡略化することが可能である．さらに，修正された指数を用いた実験により，これが実際に構造的類似性と色調的類似性の両方を評価できていることを確認した．

＜引用文献＞

[a] G. Ateniese, C. Blundo, A. D. Santis and D. R. Stinson: Extended capabilities for visual cryptography," Theoretical Computer Science 250(1-2), 143-161, 2001.
[b] Y. Desmedt, S. Hou and J.-J. Quisquater: Audio and optical cryptography, in Proceedings of Advances in Cryptology - Asiacrypt '98, Lecture Notes in Computer Science, vol. 1514, Springer-Verlag, 392-404, 1998.
[c] M. Iwamoto and H. Yamamoto: A construction method of visual secret sharing schemes for plural secret images," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E86-A(10), 2577-2588, 2003.
[d] B. Liu, R. R. Martin, J.-W. Huang and S.-M. Hu: Structure Aware Visual Cryptography, Computer Graphics Forum 33(7), 141-150, 2014.
[e] M. Naor and A. Shamir: Visual cryptography, in Proceedings of Advances in Cryptology - Eurocrypt '94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag, 1-12, 1994.
[f] W.-M. Pang, Y. Qu, T.-T. Wong, D. Cohen-Or and P.-A. Heng: Structure-aware halftoning, ACM Transactions on Graphics 27(3), 89:1-89:8, 2008.
[g] M. Sasaki and Y. Watanabe: Formulation of visual secret sharing schemes encrypting multiple images, in Proceedings of the 39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014), 7391-7395, 2014.
[h] S. J. Shyu and H.-W. Jiang: General constructions for threshold multiple-secret visual cryptographic schemes, IEEE Transactions on Information Forensics and Security 8(5), 733-743, 2013.
[i] S. Washio and Y. Watanabe: Security of audio secret sharing scheme encrypting audio secrets with bounded shares, in Proceedings of the 39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014), 7396-7400, 2014.
[j] Z. Zhou, G. R. Arce and G. D. Crescenzo: Halftone visual cryptography, IEEE Transactions on Image Processing 15(8), 2441-2453, 2006.

５．主な発表論文等

〔雑誌論文〕（計 1 件）

[1] Manami Sasaki and Yodai Watanabe: Visual secret sharing schemes encrypting multiple images, IEEE Transactions on Information Forensics and Security 13(2), 356-365, 2018. 査読有

〔学会発表〕（計 3 件）

[2] Keisuke Tamoi, Takafumi Hayashi and Yodai Watanabe: Security analysis of audio secret sharing scheme encrypting audio secrets, in Proceedings of the 7th IEEE International Conference on Awareness Science and Technology (iCAST 2015), 130-134, 2015. 査読有

[3] Yuto Miura and Yodai Watanabe: Security of (n,n)-threshold audio secret sharing schemes encrypting audio secrets, in Proceedings of the 2016 IEEE Workshop on Statistical Signal Processing (SSP 16), 646-650, 2016. 査読有

[4] Ryosuke Kawakubo and Yodai Watanabe: Simple formulation of structural similarity for halftoning and its application to visual secret sharing, in Proceedings of the 9th IEEE International Conference on Awareness Science and Technology (iCAST 2018), 106-110, 2018. 査読有

〔産業財産権〕
○取得状況（計 1 件）
名称：視覚復号型秘密画像分散法、及びこれを実行するプログラム
発明者：渡辺曜大
権利者：公立大学法人会津大学
種類：特許
番号：特許第 6391109 号
取得年：平成 30 年
国内外の別： 国内

６．研究組織

(1)研究分担者
研究分担者氏名：前田 多可雄
ローマ字氏名：Takao Maeda
所属研究機関名：会津大学
部局名：コンピュータ理工学部
職名：上級准教授
研究者番号（8 桁）：00264565