【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成27年1月29日(2015.1.29)

【公開番号】特開2013-167865(P2013-167865A)
【公開日】平成25年8月29日(2013.8.29)
【年通号数】公開・登録公報2013-046
【出願番号】特願2012-227771(P2012-227771)
【国際特許分類】
Ｇ０９Ｃ　5/00　(2006.01)
Ｈ０４Ｎ　1/387　(2006.01)
Ｇ０６Ｔ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　5/00
Ｈ０４Ｎ　1/387
Ｇ０６Ｔ　1/00　５００Ｂ

【手続補正書】
【提出日】平成26年12月8日(2014.12.8)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項８
【補正方法】変更
【補正の内容】
【請求項８】
カバーデータｃに秘密データｍが隠蔽されたステゴオブジェクトｓから秘密データｍを抽出するステガノグラフィー技術に対して、
ｎ個の参照データ$Ｉ_{1}$～$Ｉ_{n}$と、各参照データ$Ｉ_{1}$～$Ｉ_{n}$の特徴ベクトル$Ｆ_{1}$～$Ｆ_{n}$と、それぞれの参照データ$Ｉ_{1}$～$Ｉ_{n}$における貢献度$ａ_{1}$～$ａ_{n}$と、ν個（ν＞ｎ）の秘密データ$ｍ_{1}$～$ｍ_{ν}$とに基づいて、モーフィングデータを生成するモーフィング技術を適用することにより、
秘密データをステゴオブジェクトｓより復元する秘密情報復元装置であって、
カバーデータｃとして参照データ｛$Ｉ_{1}$，$Ｉ_{2}$，・・・，$Ｉ_{n}$｝を設定し、ステゴ鍵$ｋ_{s}$として特徴ベクトル｛$Ｆ_{1}$，$Ｆ_{2}$，・・・，$Ｆ_{n}$｝と貢献度｛$ａ_{1}$，$ａ_{2}$，・・・，$ａ_{n}$｝とを設定し、抽出される秘密データｍを秘密データ｛$ｍ_{1}$，$ｍ_{2}$，・・・，$ｍ_{ν}$｝として、
【数２９】

$$F_{0p}=\sum_{j=1}^{n}a_{j}F_{jp},\quad p=1,2,\ldots,N_{f}$$

を用いて、モーフィングデータの特徴ベクトル$Ｆ_{0}$を求める$Ｆ_{0}$生成手段と、
【数３０】

$$I_{j}^{w}=W(I_{j},F_{j},F_{0}),\quad j=1,2,\ldots,n$$

を用いて、各参照データ$Ｉ_{j}$（ｊ＝１，２，・・・，ｎ）の変形されたデータ$Ｉ^{ｗ}{}_{j}$（ｊ＝１，２，・・・，ｎ）を求めるデータ変形手段と、
ｐに１の値を設定し、ｑに１の値を設定して、変数ｐ及びｑの初期化を行った後に、

$\Delta_p(j_1, j_2) = (I^w_{j_1,p} - I^w_{j_2,p}) \neq 0$となる$j_1$と$j_2$とが存在するか否かを判断し、

$\Delta_p(j_1, j_2) = (I^w_{j_1,p} - I^w_{j_2,p}) \neq 0$となる$j_1$と$j_2$とが存在しない場合には、pの値を1だけ増加して、$\Delta_p(j_1, j_2) = (I^w_{j_1,p} - I^w_{j_2,p}) \neq 0$となる$j_1$と$j_2$とが存在するか否かの判断を繰り返し実行し、

$\Delta_p(j_1, j_2) = (I^w_{j_1,p} - I^w_{j_2,p}) \neq 0$となる$j_1$と$j_2$とが存在する場合に、該当する$j_1$及び$j_2$に基づいて

$m_q = s_p - MSB(s_p)$

を用いて、秘密データm_qを求め、pの値を1だけ増加し、さらに、qの値を1だけ増加して、

その後に、$q < \nu$を満たすか否かを判断し、

$q < \nu$を満たす場合には、上述した$\Delta_p(j_1, j_2) = (I^w_{j_1,p} - I^w_{j_2,p}) \neq 0$となる$j_1$と$j_2$とが存在するか否かを判断する処理に移行して当該判断処理を$q \geqq \nu$となるまで繰り返し実行することにより、

ステゴオブジェクトに隠蔽されたν個の秘密データを抽出する秘密データ再現手段と

を有し、

但し、F_{jp}（$j = 0, 1, \cdots, n$）は、F_jのp番目の要素を示し、I^w_j（$j = 1, 2, \cdots, n$）はI_jの変形を示し、Wは変形（ワーピング）関数を示し、変形関数WによりI_j（$j = 1, 2, \cdots, n$）が変形されて、I^w_j（$j = 1, 2, \cdots, n$）が生成され、I^w_j（$j = 1, 2, \cdots, n$）は、特徴ベクトルF_0を有し、また、s_p, I^0_{0p}, I^w_{1p}, $\cdots$, I^w_{np}は、それぞれ、s, I^0_0, I^w_1, $\cdots$, I^w_nのp番目の要素を示し、さらに、j_1とj_2とは、$1 \leqq j_1 < j_2 \leqq n$を満たす自然数であり、貢献度$a_j$（$j = 1, 2, \cdots, n$）の値は予め正規化され、貢献度の和の値は、$a_1 + a_2 + \cdots + a_n = 1$を満たし、また、秘密データ$m_q$（$q = 1, 2, \cdots, \nu$）は、bビットのデータであり、$\underline{s_p}$はBビットのデータであって、$MSB(s_p)$は、$s_p$のうち上位B－bビットのデータを取り出す関数を意味する

ことを特徴とする秘密情報復元装置。

【手続補正２】

【補正対象書類名】特許請求の範囲

【補正対象項目名】請求項１０

【補正方法】変更

【補正の内容】

【請求項１０】

カバーデータcに秘密データmが隠蔽されたステゴオブジェクトsから秘密データmを抽出するステガノグラフィー技術に対して、

n個の参照データ$I_1 \sim I_n$と、各参照データ$I_1 \sim I_n$の特徴ベクトル$F_1 \sim F_n$と、それぞれの参照データ$I_1 \sim I_n$における貢献度$a_1 \sim a_n$と、ν個（$\nu > n$）の秘密データ$m_1 \sim m_\nu$とに基づいて、モーフィングデータを生成するモーフィング技術を適用することにより、

秘密データをステゴオブジェクトsより復元する秘密情報復元装置であって、

カバーデータcとして参照データ$\{I_1, I_2, \cdots, I_n\}$を設定し、ステゴ鍵$k_s$として特徴ベクトル$\{F_1, F_2, \cdots, F_n\}$と貢献度$\{a_1, a_2, \cdots, a_n\}$とを設定し、抽出される秘密データmを秘密データ$\{m_1, m_2, \cdots, m_\nu\}$として、

【数３６】

$$F_{0p} = \sum_{j=1}^{n} a_j F_{jp}, \quad p = 1,2,\ldots,N_f$$

を用いて、モーフィングデータの特徴ベクトルF_0を求めるF_0生成手段と、

【数３７】

$$I_j^w = W(I_j, F_j, F_0), \quad j = 1, 2, \ldots, n$$

を用いて、各参照データI_j（ｊ＝１，２，・・・，ｎ）の変形されたデータI^w_j（ｊ＝１，２，・・・，ｎ）を求めるデータ変形手段と、

ｐに１の値を設定し、ｑに１の値を設定して、変数ｐ及びｑの初期化を行った後に、

$\Delta_p(j_1, j_2) = (I^w_{j_1,p} - I^w_{j_2,p}) \neq 0$となる$j_1$と$j_2$とが存在するか否かを判断し、

$\Delta_p(j_1, j_2) = (I^w_{j_1,p} - I^w_{j_2,p}) \neq 0$となる$j_1$と$j_2$とが存在しない場合には、ｐの値を１だけ増加して、$\Delta_p(j_1, j_2) = (I^w_{j_1,p} - I^w_{j_2,p}) \neq 0$となる$j_1$と$j_2$とが存在するか否かの判断を繰り返し実行し、

$\Delta_p(j_1, j_2) = (I^w_{j_1,p} - I^w_{j_2,p}) \neq 0$となる$j_1$と$j_2$とが存在する場合に、該当する$j_1$及び$j_2$に基づいて

【数３８】

$$m_q = (s_p - MSB(s_p)) \oplus y$$

を用いて、秘密データm_qを求め、ｐの値を１だけ増加し、さらに、ｑの値を１だけ増加して、

その後に、$q < \nu$を満たすか否かを判断し、

$q < \nu$を満たす場合には、上述した$\Delta_p(j_1, j_2) = (I^w_{j_1,p} - I^w_{j_2,p}) \neq 0$となる$j_1$と$j_2$とが存在するか否かを判断する処理に移行して当該判断処理を$q \geqq \nu$となるまで繰り返し実行することにより、

ステゴオブジェクトに隠蔽されたν個の秘密データを抽出する秘密データ再現手段と

を有し、

但し、F_{jp}（ｊ＝０，１，・・・，ｎ）は、F_jのｐ番目の要素を示し、I^w_j（ｊ＝１，２，・・・，ｎ）はI_jの変形を示し、Ｗは変形（ワーピング）関数を示し、変形関数ＷによりI_j（ｊ＝１，２，・・・，ｎ）が変形されて、I^w_j（ｊ＝１，２，・・・，ｎ）が生成され、I^w_j（ｊ＝１，２，・・・，ｎ）は、特徴ベクトルF_0を有し、また、s_p，I^0_{0p}，I^w_{1p}，・・・，I^w_{np}は、それぞれ、ｓ，I^0_0，I^w_1，・・・，I^w_nのｐ番目の要素を示し、さらに、j_1とj_2とは、$1 \leqq j_1 < j_2 \leqq n$を満たす自然数であり、貢献度$a_j$（ｊ＝１，２，・・・，ｎ）の値は予め正規化され、貢献度の和の値は、$a_1 + a_2 + \cdots + a_n = 1$を満たし、また、秘密データ$m_q$（ｑ＝１，２，・・・，ν）は、ｂビットのデータであり、$\underline{s_p}$はＢビットのデータであって、ＭＳＢ（s_p）は、s_pのうち上位Ｂ－ｂビットのデータを取り出す関数を意味し、さらに、

【数３９】

$\oplus$

は、ビット単位の排他的論理和の演算子を示し、ｙとして、I^0_0，I^w_{np}あるいは、$(I^w_{j_1,p} - I^w_{j_2,p})$のいずれかであって、ｂビットの数値からなるデータが設定される

ことを特徴とする秘密情報復元装置。

【手続補正３】

【補正対象書類名】特許請求の範囲

【補正対象項目名】請求項１８

【補正方法】変更

【補正の内容】
【請求項１８】
カバーデータｃに秘密データｍが隠蔽されたステゴオブジェクトｓから秘密データｍを抽出するステガノグラフィー技術に対して、
ｎ個の参照データI_1～I_nと、各参照データI_1～I_nの特徴ベクトルF_1～F_nと、それぞれの参照データI_1～I_nにおける貢献度a_1～a_nと、ν個（ν＞ｎ）の秘密データm_1～m_νとに基づいて、モーフィングデータを生成するモーフィング技術を適用することにより、
秘密データをステゴオブジェクトｓより復元する秘密情報復元装置の秘密情報復元プログラムであって、
カバーデータｃとして参照データ｛I_1，I_2，・・・，I_n｝を設定し、ステゴ鍵k_sとして特徴ベクトル｛F_1，F_2，・・・，F_n｝と貢献度｛a_1，a_2，・・・，a_n｝とを設定し、抽出される秘密データｍを秘密データ｛m_1，m_2，・・・，m_ν｝として、
前記秘密情報復元装置の計算手段に、
【数６８】

$$F_{0p}=\sum_{j=1}^{n}a_j F_{jp},\quad p=1,2,\ldots,N_f$$

を用いて、モーフィングデータの特徴ベクトルF_0を求めさせるF_0生成機能と、
【数６９】

$$I_j^w=W(I_j,F_j,F_0),\quad j=1,2,\ldots,n$$

を用いて、各参照データI_j（ｊ＝１，２，・・・，ｎ）の変形されたデータI^w_j（ｊ＝１，２，・・・，ｎ）を求めさせるデータ変形機能と、
ｐに１の値を設定し、ｑに１の値を設定して、変数ｐ及びｑの初期化を行った後に、
$\Delta_p(j_1,j_2)=(I^w_{j_1,p}-I^w_{j_2,p})\neq 0$となる$j_1$と$j_2$とが存在するか否かを判断させ、
$\Delta_p(j_1,j_2)=(I^w_{j_1,p}-I^w_{j_2,p})\neq 0$となる$j_1$と$j_2$とが存在しない場合には、ｐの値を１だけ増加させて、$\Delta_p(j_1,j_2)=(I^w_{j_1,p}-I^w_{j_2,p})\neq 0$となる$j_1$と$j_2$とが存在するか否かの判断を繰り返し実行させ、
$\Delta_p(j_1,j_2)=(I^w_{j_1,p}-I^w_{j_2,p})\neq 0$となる$j_1$と$j_2$とが存在する場合に、該当する$j_1$及び$j_2$に基づいて
$m_q=s_p-MSB(s_p)$
を用いて、秘密データm_qを求めさせ、ｐの値を１だけ増加させ、さらに、ｑの値を１だけ増加させて、
その後に、ｑ＜νを満たすか否かを判断させ、
ｑ＜νを満たす場合には、上述した$\Delta_p(j_1,j_2)=(I^w_{j_1,p}-I^w_{j_2,p})\neq 0$となる$j_1$と$j_2$とが存在するか否かを判断させる処理に移行して当該判断処理をｑ≧νとなるまで繰り返し実行させることにより、
ステゴオブジェクトに隠蔽されたν個の秘密データを抽出させる秘密データ再現機能と
を実現させ、
但し、F_{jp}（ｊ＝０，１，・・・，ｎ）は、F_jのｐ番目の要素を示し、I^w_j（ｊ＝１，２，・・・，ｎ）はI_jの変形を示し、Ｗは変形（ワーピング）関数を示し、変形関数ＷによりI_j（ｊ＝１，２，・・・，ｎ）が変形されて、I^w_j（ｊ＝１，２，・・・，ｎ）が生成され、I^w_j（ｊ＝１，２，・・・，ｎ）は、特徴ベクトルF_0を有し、また、s_p，I^0_{0p}，I^w_{1p}，・・・，I^w_{np}は、それぞれ、ｓ，I^0_0，I^w_1

，・・・，I^w_nのｐ番目の要素を示し、さらに、j_1とj_2とは、$1 \leqq j_1 < j_2 \leqq n$を満たす自然数であり、貢献度$a_j$（ｊ＝１，２，・・・，ｎ）の値は予め正規化され、貢献度の和の値は、$a_1+a_2+\cdots+a_n=1$を満たし、また、秘密データm_q（ｑ＝１，２，・・・，ν）は、ｂビットのデータであり、s_pはＢビットのデータであって、ＭＳＢ（s_p）は、s_pのうち上位Ｂ－ｂビットのデータを取り出す関数を意味する
ことを特徴とする秘密情報復元装置の秘密情報復元プログラム。
【手続補正４】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項２０
【補正方法】変更
【補正の内容】
【請求項２０】
カバーデータｃに秘密データｍが隠蔽されたステゴオブジェクトｓから秘密データｍを抽出するステガノグラフィー技術に対して、
ｎ個の参照データI_1～I_nと、各参照データI_1～I_nの特徴ベクトルF_1～F_nと、それぞれの参照データI_1～I_nにおける貢献度a_1～a_nと、ν個（ν＞ｎ）の秘密データm_1～m_νとに基づいて、モーフィングデータを生成するモーフィング技術を適用することにより、
秘密データをステゴオブジェクトｓより復元する秘密情報復元装置の秘密情報復元プログラムであって、
カバーデータｃとして参照データ｛I_1，I_2，・・・，I_n｝を設定し、ステゴ鍵k_sとして特徴ベクトル｛F_1，F_2，・・・，F_n｝と貢献度｛a_1，a_2，・・・，a_n｝とを設定し、抽出される秘密データｍを秘密データ｛m_1，m_2，・・・，m_ν｝として、
前記秘密情報復元装置の計算手段に、
【数７５】

$$F_{0p}=\sum_{j=1}^{n} a_j F_{jp},\quad p=1,2,\ldots,N_f$$

を用いて、モーフィングデータの特徴ベクトルF_0を求めさせるF_0生成機能と、
【数７６】

$$I_j^w=W(I_j,F_j,F_0),\quad j=1,2,\ldots,n$$

を用いて、各参照データI_j（ｊ＝１，２，・・・，ｎ）の変形されたデータI^w_j（ｊ＝１，２，・・・，ｎ）を求めさせるデータ変形機能と、
ｐに１の値を設定し、ｑに１の値を設定して、変数ｐ及びｑの初期化を行った後に、
$\Delta_p(j_1,j_2)=(I^w_{j_1,p}-I^w_{j_2,p})\neq 0$となる$j_1$と$j_2$とが存在するか否かを判断させ、
$\Delta_p(j_1,j_2)=(I^w_{j_1,p}-I^w_{j_2,p})\neq 0$となる$j_1$と$j_2$とが存在しない場合には、ｐの値を１だけ増加させて、$\Delta_p(j_1,j_2)=(I^w_{j_1,p}-I^w_{j_2,p})\neq 0$となる$j_1$と$j_2$とが存在するか否かの判断を繰り返し実行させ、
$\Delta_p(j_1,j_2)=(I^w_{j_1,p}-I^w_{j_2,p})\neq 0$となる$j_1$と$j_2$とが存在する場合に、該当する$j_1$及び$j_2$に基づいて
【数７７】

$$m_q=(S_p-MSB(S_p))\oplus y$$

を用いて、秘密データm_qを求めさせ、ｐの値を１だけ増加させ、さらに、ｑの値を１だけ増加させて、

その後に、$q<\nu$を満たすか否かを判断させ、

$q<\nu$を満たす場合には、上述した$\Delta_p(j_1, j_2)=(I^w_{j_1,p}-I^w_{j_2,p})\neq 0$となる$j_1$と$j_2$とが存在するか否かを判断させる処理に移行して当該判断処理を$q\geqq\nu$となるまで繰り返し実行させることにより、

ステゴオブジェクトに隠蔽されたν個の秘密データを抽出させる秘密データ再現機能と

を実現させ

但し、F_{jp}（$j=0, 1, \cdots, n$）は、F_jのｐ番目の要素を示し、I^w_j（$j=1, 2, \cdots, n$）はI_jの変形を示し、Ｗは変形（ワーピング）関数を示し、変形関数ＷによりI_j（$j=1, 2, \cdots, n$）が変形されて、I^w_j（$j=1, 2, \cdots, n$）が生成され、I^w_j（$j=1, 2, \cdots, n$）は、特徴ベクトルF_0を有し、また、s_p, I^0_{0p}, I^w_{1p}, ・・・, I^w_{np}は、それぞれ、ｓ, I^0_0, I^w_1, ・・・, I^w_nのｐ番目の要素を示し、さらに、j_1とj_2とは、$1\leqq j_1<j_2\leqq n$を満たす自然数であり、貢献度a_j（$j=1, 2, \cdots, n$）の値は予め正規化され、貢献度の和の値は、$a_1+a_2+\cdots+a_n=1$を満たし、また、秘密データm_q（$q=1, 2, \cdots, \nu$）は、ｂビットのデータであり、$\underline{s_p}$はＢビットのデータであって、ＭＳＢ（s_p）は、s_pのうち上位Ｂ－ｂビットのデータを取り出す関数を意味し、さらに、

【数７８】

は、ビット単位の排他的論理和の演算子を示し、ｙとして、I^0_0, I^w_{np}あるいは、$(I^w_{j_1,p}-I^w_{j_2,p})$のいずれかであって、ｂビットの数値からなるデータが設定される

ことを特徴とする秘密情報復元装置の秘密情報復元プログラム。

【手続補正５】

【補正対象書類名】明細書

【補正対象項目名】００５４

【補正方法】変更

【補正の内容】

【００５４】

また、本発明に係る秘密情報復元装置の秘密情報復元プログラムは、

カバーデータｃに秘密データｍが隠蔽されたステゴオブジェクトｓから秘密データｍを抽出するステガノグラフィー技術に対して、

ｎ個（$n\geqq 3$）の参照データI_1～I_nと、各参照データI_1～I_nの特徴ベクトルF_1～F_nと、それぞれの参照データI_1～I_nにおける貢献度a_1～a_nとに基づいて、モーフィングデータI_0を生成するモーフィング技術を適用することにより、

秘密データをステゴオブジェクトｓより復元する方法を実現するための秘密情報復元装置の秘密情報復元プログラムであって、

ステゴオブジェクトｓとして、モーフィングデータI_0を設定し、カバーデータｃとして参照データ$\{I_2, I_3, \cdots, I_n\}$を設定し、ステゴ鍵$k_s$として特徴ベクトル$\{F_1, F_2, \cdots, F_n\}$と貢献度$\{a_1, a_2, \cdots, a_n\}$とを設定し、抽出される秘密データｍを参照データ$I_1$として、

前記秘密情報復元装置の計算手段に、

【数５７】

$$F_{0p}=\sum_{j=1}^{n}a_j F_{jp},\quad p=1,2,...,N_f$$

に基づいて、モーフィングデータＩ$_0$の特徴ベクトルＦ$_0$を求めさせるＦ$_0$生成機能と、

【数５８】

$$I_j^w=W(I_j,F_j,F_0),\quad j=2,3,...,n$$

に基づいて、各参照データＩ$_j$（ｊ＝２，３，・・・，ｎ）の変形されたデータＩ^w_j（ｊ＝２，３，・・・，ｎ）を求めさせるデータ変形機能と、

【数５９】

$$I_{1p}^w=(I_{0p}-\sum_{j=2}^{n}a_j I_{jp}^w)/a_1,\quad p=1,2,...,N_d$$

に基づいて、秘密データＩ$_1$の変形されたデータＩ$^w_1$を求めさせ、

【数６０】

$$I_1=W(I_1^w,F_0,F_1)$$

に基づいて秘密データＩ$_1$を抽出させることにより、

複数の参照データに対して隠蔽された秘密データを抽出させる秘密データ再現機能とを実現させるための秘密情報復元装置の秘密情報復元プログラムであることを特徴とする。

【手続補正６】

【補正対象書類名】明細書

【補正対象項目名】００６３

【補正方法】変更

【補正の内容】

【００６３】

また、本発明に係る秘密情報復元装置の秘密情報復元プログラムは、

カバーデータｃに秘密データｍが隠蔽されたステゴオブジェクトｓから秘密データｍを抽出するステガノグラフィー技術に対して、

ｎ個の参照データＩ$_1$～Ｉ$_n$と、各参照データＩ$_1$～Ｉ$_n$の特徴ベクトルＦ$_1$～Ｆ$_n$と、それぞれの参照データＩ$_1$～Ｉ$_n$における貢献度ａ$_1$～ａ$_n$と、ν個（ν＞ｎ）の秘密データｍ$_1$～ｍ$_ν$とに基づいて、モーフィングデータを生成するモーフィング技術を適用することにより、

秘密データをステゴオブジェクトｓより復元する方法を実現するための秘密情報復元装置の秘密情報復元プログラムであって、

カバーデータｃとして参照データ｛Ｉ$_1$，Ｉ$_2$，・・・，Ｉ$_n$｝を設定し、ステゴ鍵ｋ$_s$として特徴ベクトル｛Ｆ$_1$，Ｆ$_2$，・・・，Ｆ$_n$｝と貢献度｛ａ$_1$，ａ$_2$，・・・，ａ$_n$｝とを設定し、抽出される秘密データｍを秘密データ｛ｍ$_1$，ｍ$_2$，・・・，ｍ$_ν$｝として、

前記秘密情報復元装置の計算手段に、

【数６９】

$$F_{0p}=\sum_{j=1}^{n}a_j F_{jp},\quad p=1,2,\ldots,N_f$$

を用いて、モーフィングデータの特徴ベクトルＦ$_0$を求めさせるＦ$_0$生成機能と、

【数７０】

$$I_j^w=W(I_j,F_j,F_0),\quad j=1,2,\ldots,n$$

を用いて、各参照データＩ$_j$（ｊ＝１，２，・・・，ｎ）の変形されたデータＩ$^w{}_j$（ｊ＝１，２，・・・，ｎ）を求めさせるデータ変形機能と、

ｐに１の値を設定し、ｑに１の値を設定して、変数ｐ及びｑの初期化を行った後に、

Δ$_p$（ｊ$_1$，ｊ$_2$）＝（Ｉ$^w{}_{j_1,p}$－Ｉ$^w{}_{j_2,p}$）≠０となるｊ$_1$とｊ$_2$とが存在するか否かを判断させ、

Δ$_p$（ｊ$_1$，ｊ$_2$）＝（Ｉ$^w{}_{j_1,p}$－Ｉ$^w{}_{j_2,p}$）≠０となるｊ$_1$とｊ$_2$とが存在しない場合には、ｐの値を１だけ増加させて、Δ$_p$（ｊ$_1$，ｊ$_2$）＝（Ｉ$^w{}_{j_1,p}$－Ｉ$^w{}_{j_2,p}$）≠０となるｊ$_1$とｊ$_2$とが存在するか否かの判断を繰り返し実行させ、

Δ$_p$（ｊ$_1$，ｊ$_2$）＝（Ｉ$^w{}_{j_1,p}$－Ｉ$^w{}_{j_2,p}$）≠０となるｊ$_1$とｊ$_2$とが存在する場合に、該当するｊ$_1$及びｊ$_2$に基づいて

ｍ$_q$＝ｓ$_p$－ＭＳＢ（ｓ$_p$）

を用いて、秘密データｍ$_q$を求めさせ、ｐの値を１だけ増加させ、さらに、ｑの値を１だけ増加させて、

その後に、ｑ＜νを満たすか否かを判断させ、

ｑ＜νを満たす場合には、上述したΔ$_p$（ｊ$_1$，ｊ$_2$）＝（Ｉ$^w{}_{j_1,p}$－Ｉ$^w{}_{j_2,p}$）≠０となるｊ$_1$とｊ$_2$とが存在するか否かを判断させる処理に移行して当該判断処理をｑ≧νとなるまで繰り返し実行させることにより、

ステゴオブジェクトに隠蔽されたν個の秘密データを抽出させる秘密データ再現機能とを実現させるための秘密情報復元装置の秘密情報復元プログラムであることを特徴とする。

【手続補正７】

【補正対象書類名】明細書

【補正対象項目名】００６４

【補正方法】変更

【補正の内容】

【００６４】

但し、Ｆ$_{jp}$（ｊ＝０，１，・・・，ｎ）は、Ｆ$_j$のｐ番目の要素を示す。Ｉ$^w{}_j$（ｊ＝１，２，・・・，ｎ）はＩ$_j$の変形を示し、Ｗは変形（ワーピング）関数を示し、変形関数ＷによりＩ$_j$（ｊ＝１，２，・・・，ｎ）が変形されて、Ｉ$^w{}_j$（ｊ＝１，２，・・・，ｎ）が生成され、Ｉ$^w{}_j$（ｊ＝１，２，・・・，ｎ）は、特徴ベクトルＦ$_0$を有する。また、ｓ$_p$，Ｉ$^0{}_{0p}$，Ｉ$^w{}_{1p}$，・・・，Ｉ$^w{}_{np}$は、それぞれ、ｓ，Ｉ$^0{}_0$，Ｉ$^w{}_1$，・・・，Ｉ$^w{}_n$のｐ番目の要素を示す。さらに、ｊ$_1$とｊ$_2$とは、１≦ｊ$_1$＜ｊ$_2$≦ｎを満たす自然数であり、貢献度ａ$_j$（ｊ＝１，２，・・・，ｎ）の値は予め正規化され、貢献度の和の値は、ａ$_1$＋ａ$_2$＋・・・＋ａ$_n$＝１を満たす。また、秘密データｍ$_q$（ｑ＝１，２，・・・，ν）は、ｂビットのデータであり、ｓ$_p$はＢビットのデータであって、ＭＳＢ（ｓ$_p$）は、ｓ$_p$のうち上位Ｂ－ｂビットのデータを取り出す関数を意味する。

【手続補正８】

【補正対象書類名】明細書

【補正対象項目名】００７２
【補正方法】変更
【補正の内容】
【００７２】
但し、F_{jp}（ｊ＝０，１，・・・，ｎ）は、F_jのｐ番目の要素を示す。$I^{w}{}_{j}$（ｊ＝１，２，・・・，ｎ）はI_jの変形を示し、Ｗは変形（ワーピング）関数を示し、変形関数ＷによりI_j（ｊ＝１，２，・・・，ｎ）が変形されて、$I^{w}{}_{j}$（ｊ＝１，２，・・・，ｎ）が生成され、$I^{w}{}_{j}$（ｊ＝１，２，・・・，ｎ）は、特徴ベクトルF_0を有する。また、s_p，$I^{0}{}_{0p}$，$I^{w}{}_{1p}$，・・・，$I^{w}{}_{np}$は、それぞれ、ｓ，$I^{0}{}_{0}$，$I^{w}{}_{1}$，・・・，$I^{w}{}_{n}$のｐ番目の要素を示す。さらに、j_1とj_2とは、$1 \leqq j_1 < j_2 \leqq n$を満たす自然数であり、貢献度$a_j$（ｊ＝１，２，・・・，ｎ）の値は予め正規化され、貢献度の和の値は、$a_1+a_2+\cdots+a_n=1$を満たす。また、秘密データm_q（ｑ＝１，２，・・・，ν）は、ｂビットのデータであり、$\underline{s_p}$はＢビットのデータであって、ＭＳＢ（s_p）は、s_pのうち上位Ｂ－ｂビットのデータを取り出す関数を意味する。さらに、
【数８６】

$$\oplus$$

は、ビット単位の排他的論理和の演算子を示し、ｙとして、$I^{0}{}_{0}$，$I^{w}{}_{np}$あるいは、（$I^{w}{}_{j1,p}-I^{w}{}_{j2,p}$）のいずれかであって、ｂビットの数値からなるデータが設定される。